CONFIGURATION MIGRATION TOOL

FortiConverter User Guide

VERSION 4.8

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Monday, October 19, 2015

FortiConverter 4.8 User Guide

1st Edition

TABLE OF CONTENTS

Introduction **6**
- SFTP service for submitting configuration files 6
- Supported vendors & configuration objects 7
- Licensing 9
- System requirements 9

What's new **10**

Installing the software **12**

Uploading the license **13**

Conversion **17**
- Downloading the source configuration files 17
  - Alcatel-Lucent 17
  - Check Point 18
  - Cisco 19
  - Fortinet 19
  - Juniper 19
  - Palo Alto Networks 20
  - SonicWall 20
- Using the conversion wizards 20
- Alcatel-Lucent conversion wizard 21
  - Start Options 21
  - Source Configuration Selection 22
  - Device Selection 23
  - Partition & Zone Rule Selection 24
  - Physical Interface Mapping 25
  - VLAN and Loopback 26
  - Route Information 27
  - Conversion Result 28
- Check Point conversion wizard 28
  - Including object comments in the output configuration 28
  - Start Options 29
  - Start Options - More 30
  - MDS Source Configuration (Provider-1 only) 32
  - MDS Selection (Provider-1 only) 33
  - Global Policy Collection Selection (Provider-1) 34

Domain Source Configuration 35
Policy Collection Selection 36
Firewall Selection (SmartCenter only) 37
Physical Interface Mapping (SmartCenter only) 38
Route Information (SmartCenter only) 39
Conversion Result 40
Cisco conversion wizard 41
Start Options 41
Source Configuration Selection 42
Context Selection 43
Physical Interface Mapping 44
VLAN and Loopback 45
Route Information 46
VPN Phase2 47
Conversion Result 48
Fortinet conversion wizard 49
Start Options 49
Source Configuration Selection 50
VDOM Selection 51
Physical Interface Mapping 52
Additional Rule 53
Conversion Result 54
Juniper conversion wizard 55
Start Options 55
Source Configuration Selection 56
LSYS (Junos OS) or VSYS (ScreenOS) Selection 57
Physical Interface Mapping 58
Route Information 59
Conversion Result 60
Palo Alto conversion wizard 61
Start Options 61
Source Configuration Selection 62
VSYS Selection 63
Physical Interface Mapping 64
Conversion Result 65
SonicWall conversion wizard 65
Start Options 66
Source Configuration Selection 67
Physical Interface Mapping 68
VLAN and Loopback 69
Route Information 70
Conversion Result 71

Snort conversion wizard 72
Start Options 72
Rule Variables 73
Conversion Result 74
Using retail branch batch conversion mode 74
Batch mode for Cisco, Juniper, Palo Alto Networks, and SonicWall firewalls 75
Batch mode for Alcatel-Lucent and Check Point firewalls 76
Viewing the results of your automatic conversion 79
Tuning the FortiConverter output 81
Toolbar options 81
Policy Tuning tab 82
NAT Merge Review tab 86
Conversion log tab 89
Importing your new configuration into FortiManager 91
Output from conversion to FortiManager 91
Import your new configuration into FortiManager 92
Understanding your new configuration 96
Alcatel-Lucent differences 96
Conversion support 96
Address and address group configuration 96
Interface configuration 96
Service and Service Group configuration 96
Policy configuration 96
VDOM configuration 98
Example conversion 98
Check Point differences 100
General 100
Schedule configuration 100
NAT and policy configuration 100
VPN configuration 101
Service objects 101
Cisco IOS, PIX or ASA differences 101
Juniper ScreenOS or Junos OS differences 102
Palo Alto Networks OS (PAN-OS) differences 102
Conversion support 102
Configuration notes 103

Introduction

This document shows how to install and use FortiConverter.

FortiConverter is designed to help you migrate your network to Fortinet network security solutions, significantly reducing workload and minimizing errors. FortiConverter translates configuration files from other vendors' firewall products into a valid FortiGate or FortiManager configuration file. Because the output uses command line syntax, it can either be uploaded as a configuration file or piped to the CLI.

For additional assistance, please contact fconvert_feedback@fortinet.com.

SFTP service for submitting configuration files

FortiConverter customers can securely submit firewall configuration files to Fortinet Engineering using Fortinet's SFTP service.

Because this account has many restrictions, Fortinet recommends that you use a command-line SFTP client to transfer files. For example, Cygwin provides a suitable SFTP client for Windows users.

To upload a file

1. Connect to the SFTP using the following settings:

Server	ftp.apsecure.com
Port	2222
User	fcon-incoming
Password	incoming

2. Create a folder using your FortiConverter serial number for its name.
3. Post your files in the new folder.

Example connection

```
sftp -P 2222 fcon-incoming@ftp.apsecure.com
$ sftp -P 2222 fcon-incoming@ftp.apsecure.com
fcon-incoming@ftp.apsecure.com's password:
Connected to ftp.apsecure.com.
sftp> ls
remote readdir("/home/fcon/incoming"): Permission denied
sftp> mkdir FCON010000010864
sftp> cd FCON010000010864
sftp> pwd
Remote working directory: /home/fcon/incoming/FCON010000010864
sftp> put config.rar
Uploading config.rar to /home/fcon/incoming/FCON010000010864/config.rar
config.rar 100% 3826KB 273.3KB/s 00:14
sftp> ls
```

```
config.rar
sftp> bye
```

Supported vendors & configuration objects

FortiConverter can translate configurations from the following vendors and platforms.

In some cases, FortiConverter cannot translate some parts of the configuration because of dependencies or unsupported syntax and you must manually convert them.

If the number of objects exceeds the maximum valid length for FortiGate or FortiManager, FortiConverter trims them.

Vendor	Models	Versions	Convertible objects
Alcatel-Lucent	Brick	v9.x	Addresses & Address Books Interfaces (physical, logical, loopback, PPPoE) Partitions Services & Service Books Static routes Zone rule set
Check Point	SmartCenter Provider-1	NG FP1 (4.) to NGX R64/R71/R75/R76	Addresses & Address Groups Interfaces (Physical, Logical, Loopback, PPPoE) Local Users & Groups NAT (Automatic & Rule) Negate Cell Policies (rulebases.fws) RADIUS, TACACS+, & LDAP Rules Schedules Services & Service Groups Static routes VPN (IPSec)
Cisco	PIX ASA FWSM	4.x to 8.x	ACLs Addresses & Address Groups DHCP Servers DNS Servers Interfaces (Physical, Logical, Loopback, PPPoE, Tunnel) IP Pools Local Users & Groups NAT (including Object NAT and Double NAT) RADIUS, TACACS+, & LDAP Services & Service Groups Static Routes Time Ranges VPN (IPSec, PPTP/L2TP, EZVPN)
	IOS	10.x to 12.x 15.x	

Vendor	Models	Versions	Convertible objects
Juniper	SSG	ScreenOS/Junos OS 5.x to 6.x	Addresses & Address Groups & FQDNs DHCP Servers & Clients & Relays Interfaces (Physical, Logical, Loopback, PPPoE, Tunnel) Static Routes Services & Service Groups Policies VIPs/MIPs NAT IP Pools VPN (IPSec, PPTP/L2TP) Local Users & Groups RADIUS & LDAP Zones
	SRX	Junos OS 10.x, 11.x, 12.x	Addresses & Address Groups & FQDNs DHCP Servers & Client & Relay Interfaces (Physical, Logical, Loopback, PPPoE, Tunnel) IP Pools Local Users & Groups NAT Policies RADIUS & LDAP Services & Service Groups Static Routes VIPs/MIPs VPN (IPSec, PPTP/L2TP) Zones
Palo Alto Networks	PA	PAN-OS 1.x to 6.x	Addresses & Address Groups & FQDNs Interfaces Local Users & Groups NAT (partial) Policies Schedules Static Routes Services & Service Groups Zones
SonicWall	NSA Serials	SonicOS Enhanced 5.x	Addresses & Address Groups & FQDNs DHCP Servers & Clients & Relays Interfaces (Physical, Logical, Loopback, PPPoE) Local Users & Groups NAT Policies Schedules Services & Service Groups Static Routes Zones

Licensing

The trial version of FortiConverter provides full conversion functionality for FortiGate-to-FortiGate conversions. It supports trial conversions for Cisco, Check Point, and Juniper. Trial conversions allow you to review of conversion results and generate 100 lines of configuration output, but the fine-tuning features are disabled.

The trial version does not support Alcatel-Lucent, Snort, Sonicwall, and Palo Alto Network conversions.

After you purchase and upload a license, FortiConverter is unlocked and full conversion functionality is enabled for all supported vendors. Your paid license entitles you to any new versions of FortiConverter that Fortinet releases until the license expires.

FortiConverter requires an Internet connection to verify its license. You can use the software for up to 30 days without validating the license online.

For more information, see "Uploading the license" on page 13

System requirements

FortiConverter requires one of the following operating systems:

- Microsoft Windows 10
- Microsoft Windows 8 (32-bit or 64-bit)
- Microsoft Windows 7 (32-bit or 64-bit)
- Microsoft Windows Server 2008 (32-bit or 64-bit)

In addition, FortiConverter requires .NET Framework 4.0. If it is not already installed on your computer, the FortiConverter installer prompts you to download and install it.

A web browser is required to view conversion reports.

An Internet connection is required to verify the software license.

What's new

The following list contains features that are new or enhanced since FortiConverter 4.4.

FortiConverter 4.8

- **Check Point conversion**
  - **Comment fields** – New options allow you to convert Check Point interface, address, service, and rule comments.
  - **Review memo** – You can now export NAT merge converted policies as a separate file for review purposes.
  - **NAT conversion** – FortiConverter now supports the conversion of both manual and automatic NAT rules and both static and hide NAT types.
  - **NAT merge review** – The tuning features for Check Point conversions now include a NAT Merge Review tab. Use it to review how FortiConverter merged NAT and firewall polices to create corresponding FortiOS policies.
  - **Service protocol type** – FortiConverter now supports the conversion of Check Point service object definitions that include a protocol type by using a FortiOS session helper.
- **Cisco conversion**
  - **Virtual contexts** – Virtual contexts are now supported. You can select individual virtual contexts to convert to equivalent VDOMs.
  - **PIX conversion** – FortiConverter now supports the conversion of Static, Policy, and Dynamic NAT and Port Address Translation (PAT) for PIX configurations.
- **Fortinet conversion**
  - **New conversion targets** – You can now select FortiOS v5.0 or v5.2 as the target for FortiGate-to-FortiGate conversions.
  - **Restorable configuration** – A new option allows you to generate configuration files that can be directly restored to the target device.
- **Juniper conversion**
  - **Enhanced conversion logic for ScreenOS** – FortiConverter now supports conversion of additional configuration objects, including redundant and VLAN1 interfaces and HA configuration.
  - **MS-RPS and SUN-RPC conversion for JunOS** – FortiConverter now supports the conversion of MS-RPS and SUN-RPS firewall services.
- **Reload exported result** – Use the Tuning button on any wizard page to load any conversion result that you exported earlier.
- **Context-sensitive help** – Click the Help button to display online help information for the current FortiConverter page in your web browser.

FortiConverter 4.7

- **Junos OS NAT merge review** — FortiConverter can now perform a NAT merge between security rules and NAT tables based on address comparison. The NAT tuning page now provides details about the conversion logic for FortiGate NAT policies. See NAT Merge Review tab on page 86
- **FortiOS 4.x to 5.x conversion** — FortiConverter now supports a limited conversion from FortiOS 4.x to FortiOS 5.x. See Fortinet conversion wizard on page 49.

- **Junos OS Logical System (LSYS) and ScreenOS Virtual System (VSYS)** — FortiConverter converts LSYS and VSYS to FortiGate VDOMs. See Juniper conversion wizard on page 55.
- **Save Fortinet conversions using the trial version** — You do not need to upload a paid license for FortiConverter before you can save your Fortinet-to-Fortinet conversions.
- **Results page web UI enhancements** — The wizard's Conversion Result page is now grouped into categories for quick review. An Export button allows you to save conversion statistics as an HTML page. For more information, see the wizard information for the vendor you want to convert.
- **Policy review wizard page** — This additional page displays detailed address/service object list information. See Policy Tuning tab on page 82.
- **Import instructions** — The conversion headers of FortiConverter output files now provide instructions for building the new configuration file. For FortiGate-to-FortiGate conversions, you simply restore the outputs, and for Snort conversions, you import the outputs.

FortiConverter 4.6

- **FortiGate to FortiGate conversion** — Move a configuration to one or more FortiGate devices using either Migrate or Split VDOMs mode. See Fortinet conversion wizard on page 49.
- **Partition and zone selection in Lucent Brick conversions** — You can select or deselect individual partitions and zones when you convert.
- **Generate NAT rules and mappings from Hide NATs in Check Point conversions** — Use Hide NATs to create the NAT rules and mappings that are specified by the `central-nat` CLI commands in FortiGate. To use, select ***Enable Central NAT merge*** on the Start Options page.
- **Auto-generate interface policies using the route table in Check Point conversions** — To use, select ***Auto generate policy interfaces*** on the Start Options page, and then add a route file on the Firewall Selection page.
- **Export or import interface maps** — You can now save and restore interface assignments.
- **Export or import tuning snapshots** — You can now save post-conversion tuning changes.

FortiConverter 4.5

- **Palo Alto Networks firewall conversion** — FortiConverter can now convert a Palo Alto Networks firewall configuration to a FortiOS configuration. See "Supported vendors & configuration objects" on page 7.
- **Batch mode for retail branch conversion** — You can now convert a group of firewalls using a single operation. See "Using retail branch batch conversion mode" on page 74.
- **Automatically check for updates** — You can configure FortiConverter to automatically check for software updates.
- **Configurable policy index values** — You can now select the initial policy number that FortiConverter uses in a converted configuration. See "Tuning the FortiConverter output" on page 81.
- **Output file directory** — FortiConverter now saves converted configurations as files in a directory with the name of the input file. If subsequent input files have a different name, it preserves any previous output files.

Installing the software

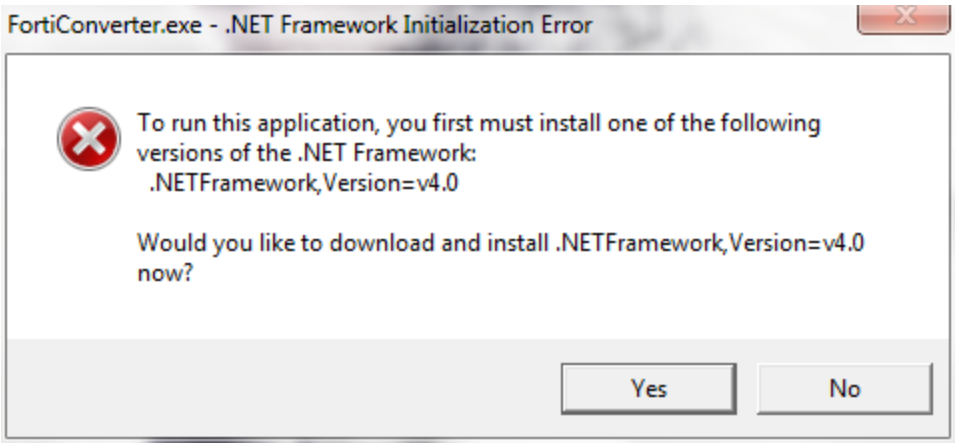
To download the FortiConverter installer from the Fortinet Technical Support web site, go to:

https://support.fortinet.com

To install FortiConverter

1. Double-click the FortiConverter installer executable (.exe).

   If your computer does not have Microsoft .NET Framework 4.0, you are prompted to install it.



2. To proceed with the installation, click **Yes** and then download the software framework from Microsoft's web site.
3. To continue the installation, read the license agreement, select **I accept the terms of the License Agreement**, and then click **Next**.
4. If you want to install the program in a location that is different from the default one, click **Browse** and select the directory.
5. Click **Next**.
6. Select the Start Menu folder that you want to add the program shortcuts to, and then click **Install**.
7. Click **Finish** to exit the FortiConverter installer.

Uploading the license

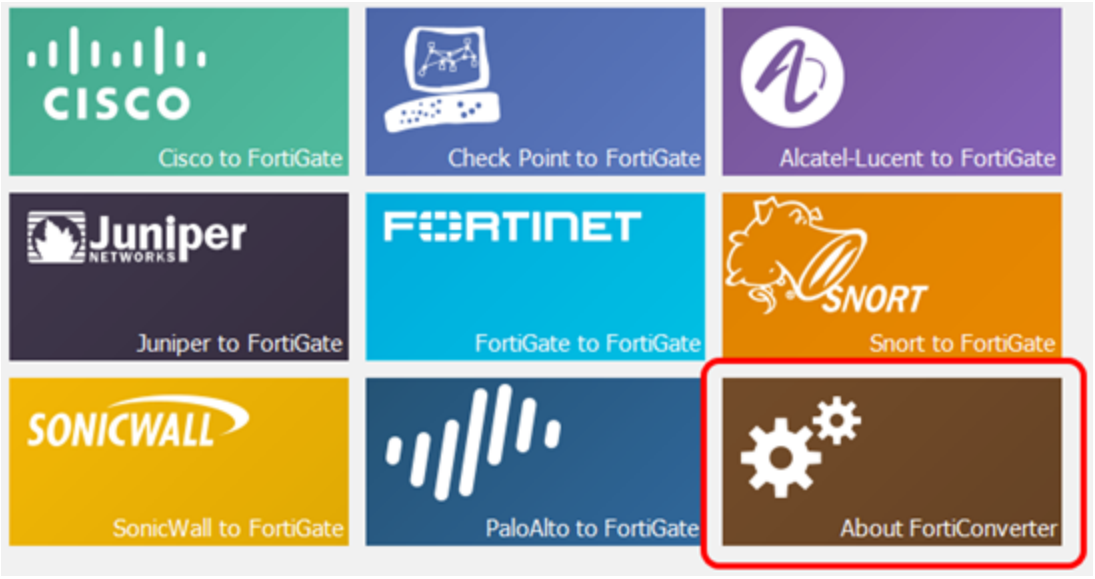
By default, FortiConverter is installed with a limited, trial license. If you have purchased an full license, upload it to unlock the complete feature set.

To purchase a license, use your usual Fortinet sales channel.

To activate the license

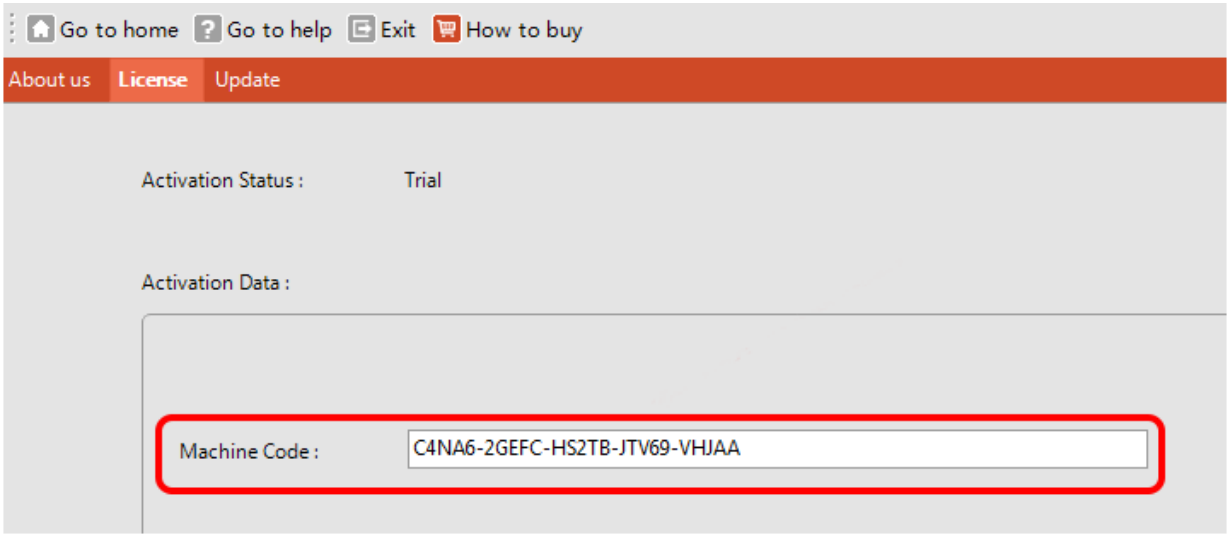
1. To start FortiConverter, double-click its shortcut.

2. Click **About FortiConverter**.



3. Click the **License** tab.

4. Copy the **Machine Code** value to the clipboard.



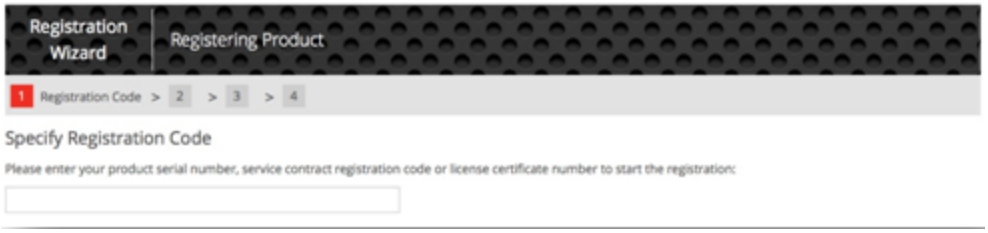
5. Ensure you have purchased a license, and then sign in to the Fortinet Technical Support web site at the following location:

   https://support.fortinet.com/

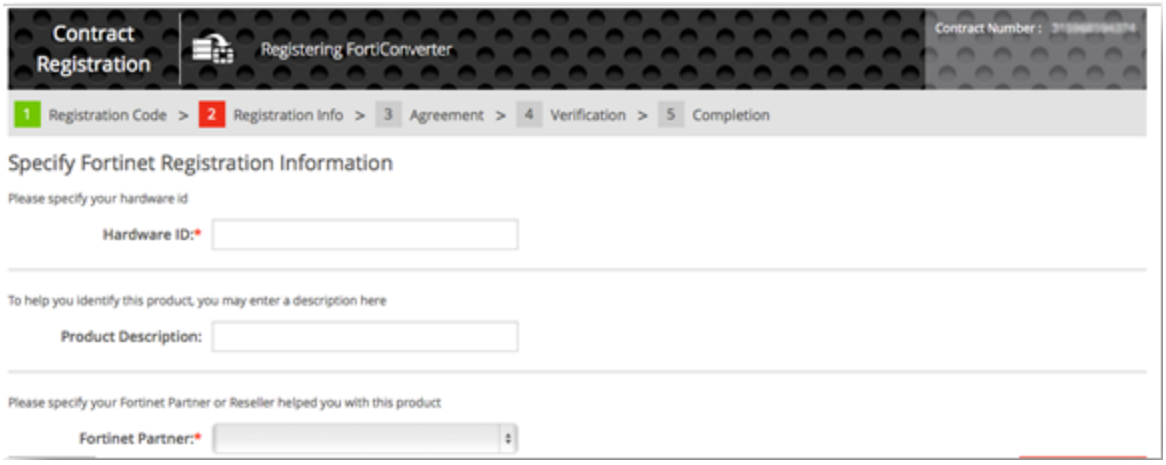
   Registration uses a simple, four-step wizard that is common to many Fortinet products.

6. On the first page of the wizard, for the registration code, enter the SKU for your FortiConverter product.

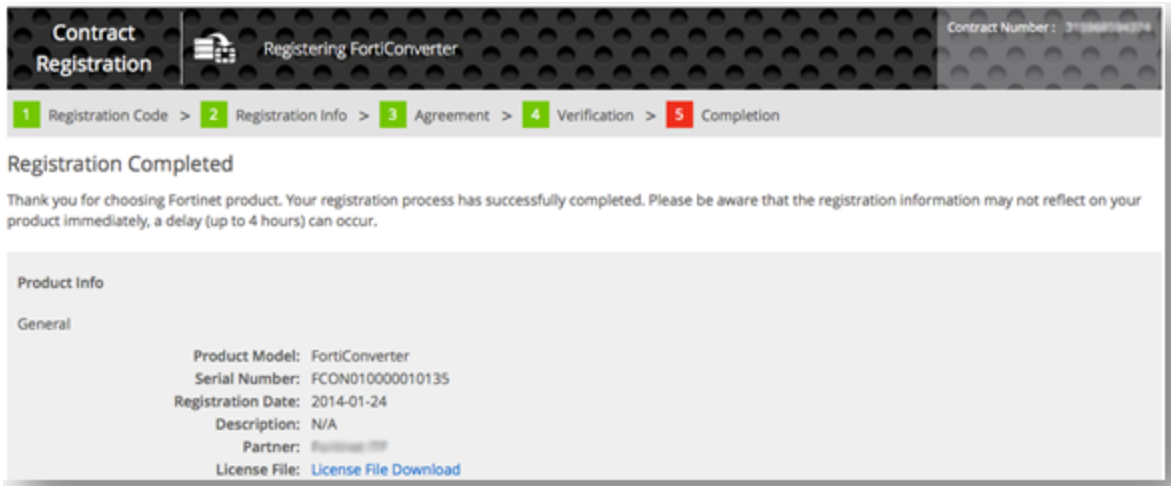
   The FortiConverter release notes provide the SKUs (go to docs.fortinet.com/forticonverter).



7. For step 2 of the registration wizard, for **Hardware ID**, enter the **Machine Code** value you copied earlier.



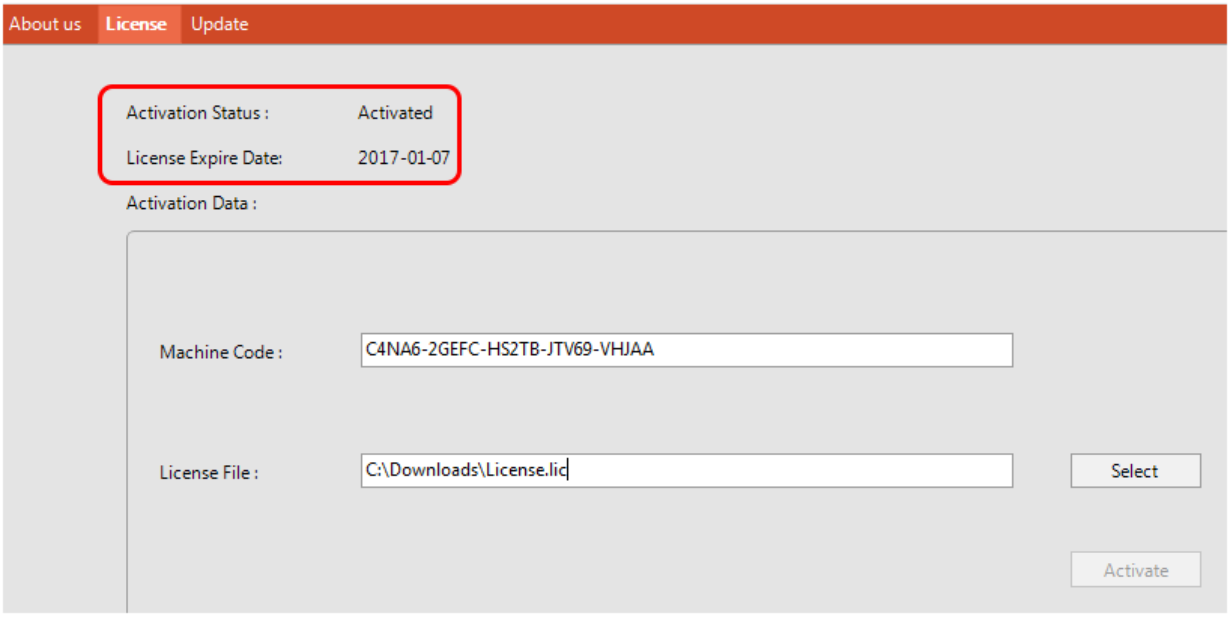
8. After you agree to the license terms, the final page of the wizard (step 5) allows you to download the license file (.lic file).



9. In FortiConverter, on the License tab, click **Select** and navigate to the .lic file to select it.

10. Click **Activate**.

    FortiConverter validates the license file and changes the value of **Activation Status** from **Free** to **Activated**.



Your license is valid for all FortiConverter software updates released until the **Expire Date** value.

After the license is activated, to access the expiry information, on the home page, click **System Setting**, and then click the **License** tab.

Conversion

FortiConverter provides wizards that convert configuration files from a specific vendor to FortiGate or FortiManager configuration files. After you input information about your previous vendor's configuration files, you can preview and fine-tune the conversion before you output the final FortiGate or FortiManager configuration file.

Downloading the source configuration files

Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed. Procedures vary by vendor.

Some vendors divide the configuration into multiple files, so make sure that you download all files.

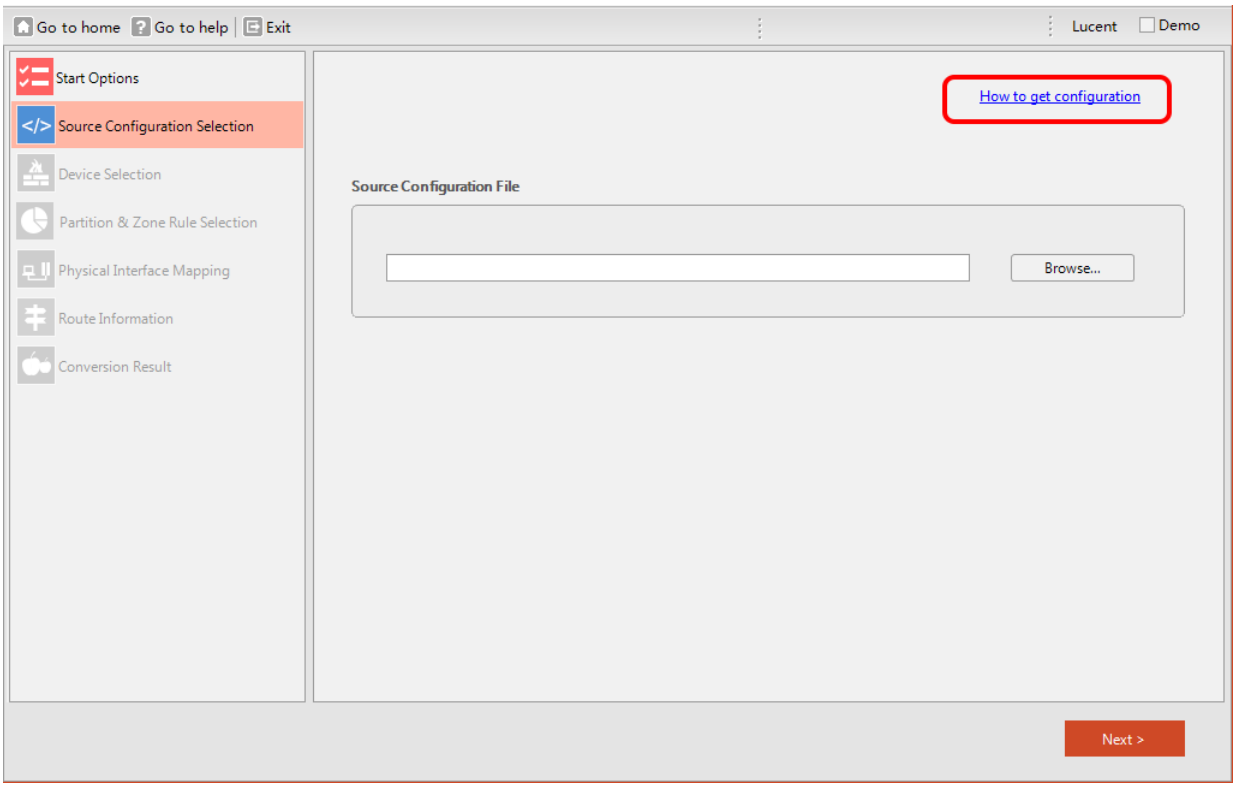
Alcatel-Lucent

FortiConverter provides a Perl script for downloading Alcatel-Lucent Brick configurations.

To access the Alcatel-Lucent configuration download script

1. On the FortiConverter home page, click the Alcatel-Lucent square.
2. On the Start Options page, click **Next**.

   If you are using the wizard to retrieve the download script only, use the default settings for this page. You can restart the wizard later after you have the file and are ready to perform the conversion with the appropriate settings.
3. On the Source Configuration Selection page, click **How to get configuration**.



The Windows folder that contains the Perl script and the documentation for using it are displayed. Follow the instructions to run the Perl script and output the source configuration as a set of directories.

Check Point

To acquire the configuration, download the following files. In most cases, you download the object and policy definitions from the management system:

- Object definitions — 'objects_5_0.C' (Check Point NG/NGX) or 'objects.C' (Check Point 4.x) contain the firewall's object definitions. To convert from Provider-1, 'mcss.C' contains the MDS hierarchy files.
- Policy and rule definitions — '*.w' or 'rulebases_5_0.fws'. The file name is <rule>.W (default Standard.W). or rulebases_5_0.fws. They are located in the directory "[SmartCenter] : $FWDIR/conf".
- Route information (optional) — Helps FortiConverter to correctly interpret the network topology being converted. To get this data, enter the `route print` command on the firewall node, and then copy and paste the output into a plain text file. Codes in the output indicate if the route is a directly connected interface, a host route, a network route, and so on. The output varies by the platform.
- User and user groups file (optional) — fwauth.NDBx

File	File name	Path
Object definitions	objects_5_0.C (Checkpoint NG/NGX) objects.C (Checkpoint 4.x_)	$FWDIR/conf

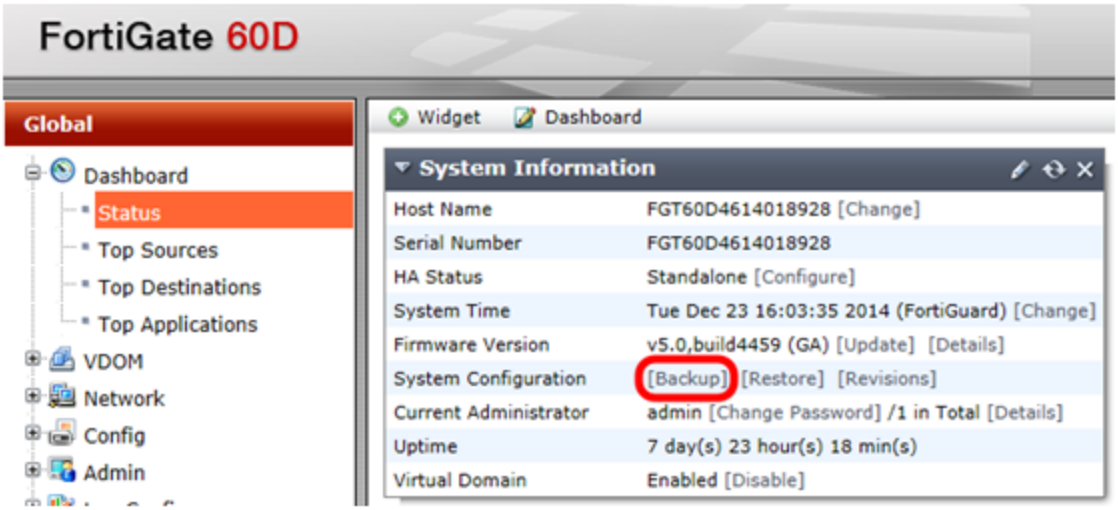
File	File name	Path
	mcss.C (Provider-1)	$MDSDIR/conf/mdsdb
Policy and Rule definitions	rulebase_5_0.fws [package name].W	$FWDIR/conf
Route information	NA	Save output of route print command from firewall
User and User Group file	fwauth.NDBx	$FWDIR/conf/ or $FWDIR/database/

Cisco

To acquire the configuration, enter the `show running-config` command, and then paste the output into a plain text file.

Fortinet

Go to **Configuration > Update > ConfigFile**. Use the web UI to download the configuration.



Juniper

To obtain the configuration, use one of the following methods:

- In the web UI, go to **Configuration > Update > ConfigFile**.
- Using the CLI, paste the output of the `get conf` command into a plain text file.

Palo Alto Networks

In the web UI, go to **Device > Setup > Operations**, and then click **Export named configuration snapshot**.

SonicWall

To download the configuration (*.exp file), in the web UI, go to **System > Settings > Export Settings**.

Using the conversion wizards

To access the conversion wizards, from the main FortiConverter window, click the appropriate icon.

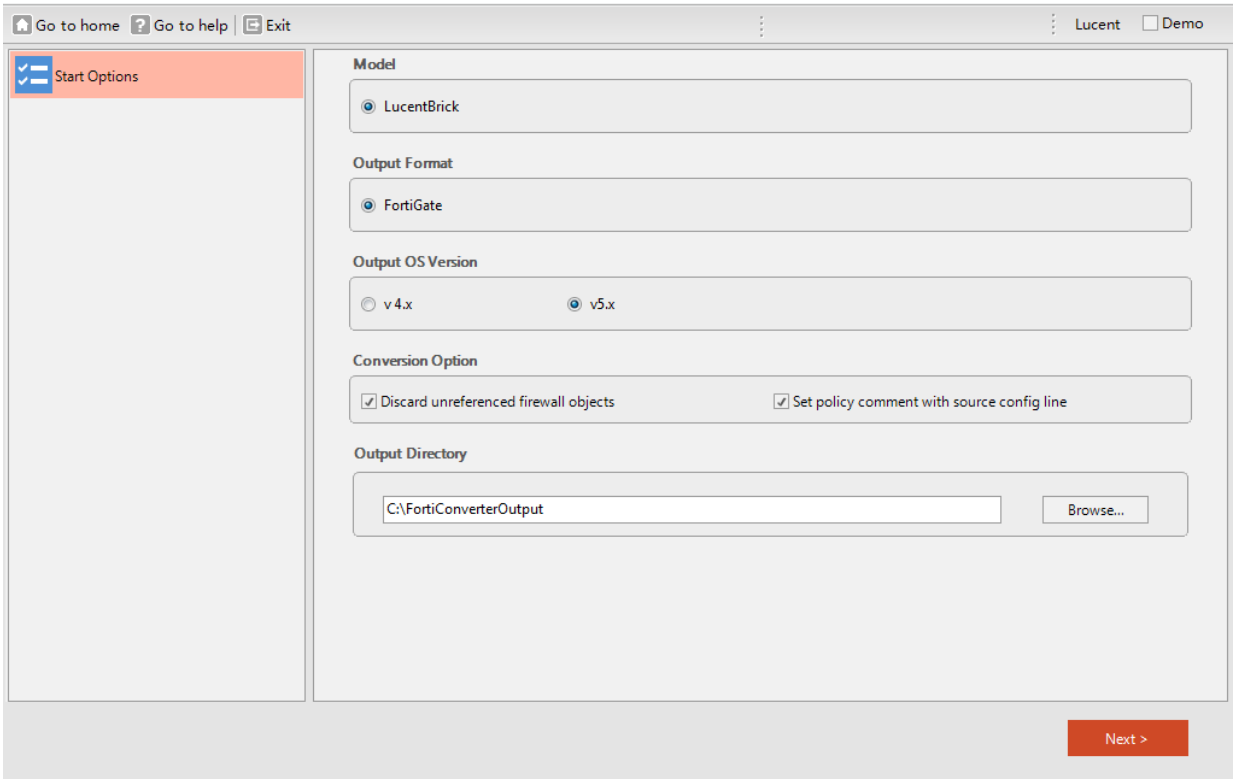
FortiConverter has a separate wizard for each supported vendor. The settings for each wizard type are described in the sections that follow this introduction.

Each wizard has a demo configuration file that can be selected using the Demo check box in the upper right corner.

The settings that are displayed depend the input configuration. For some conversions, not every page in the wizard is displayed.

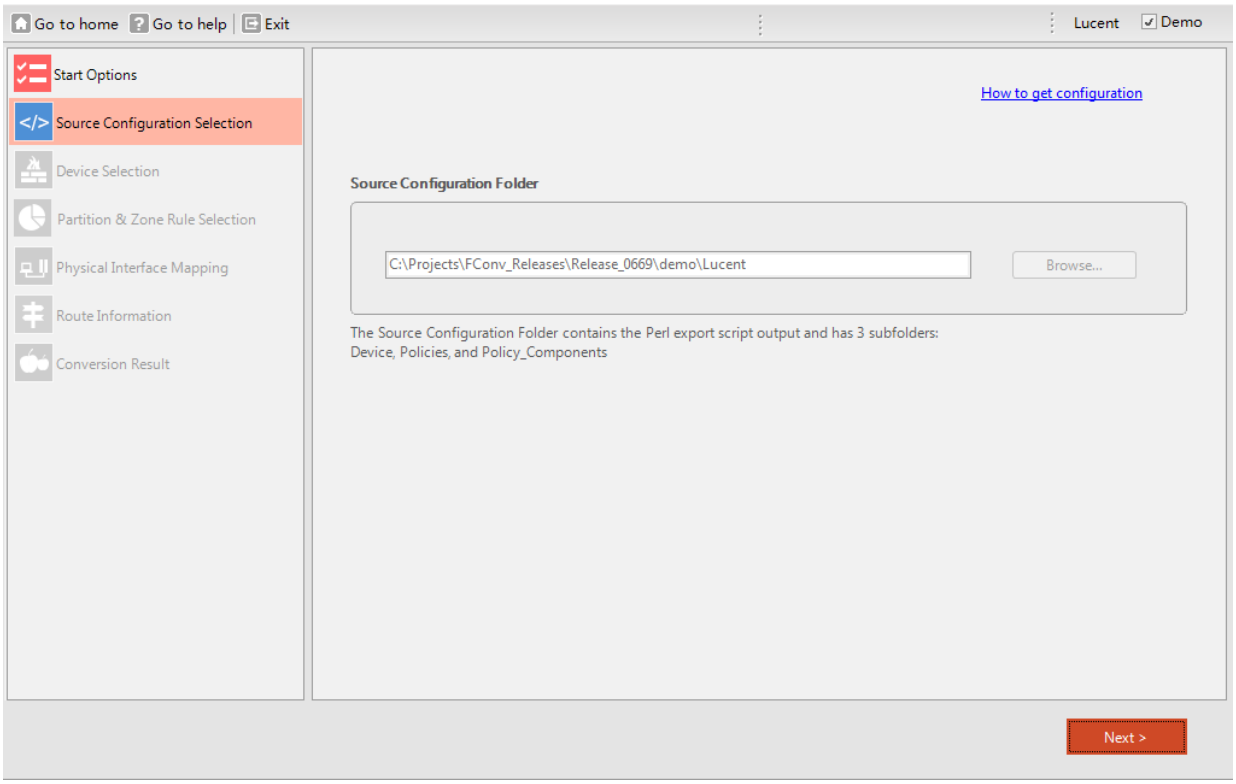
Alcatel-Lucent conversion wizard

Start Options



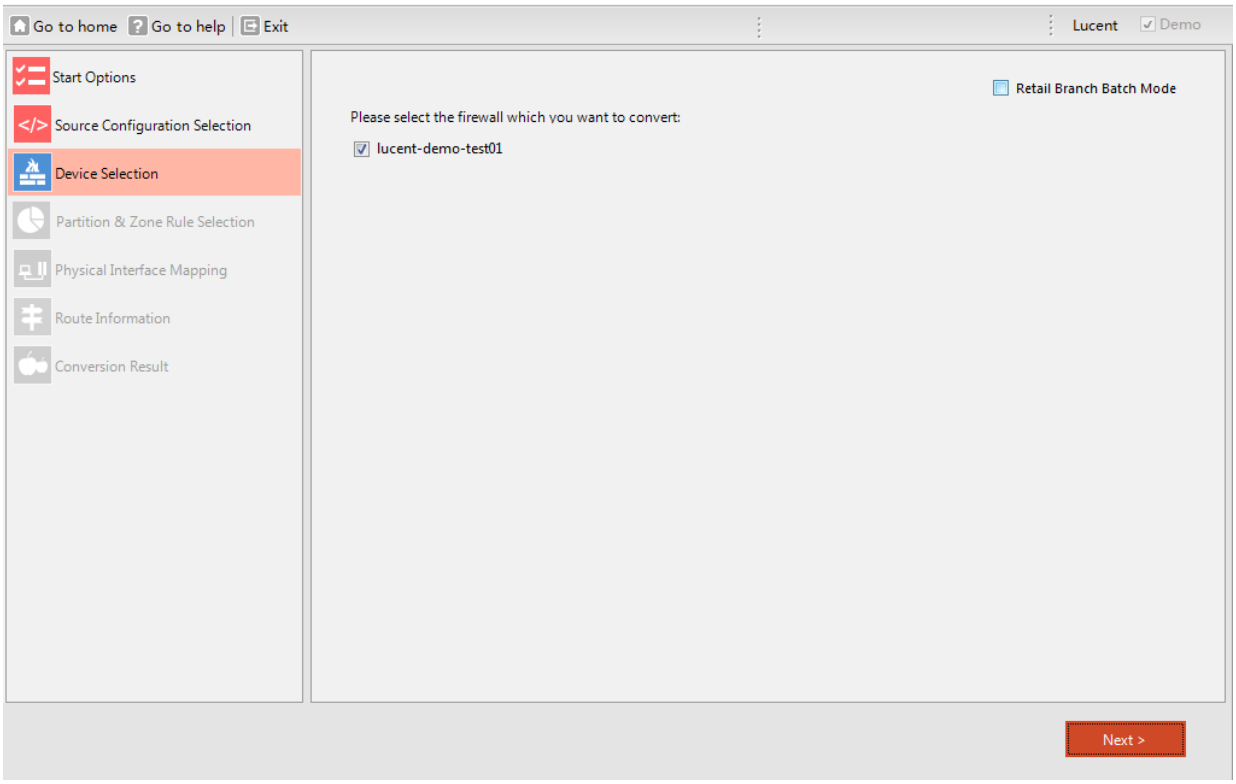
Setting	Description
Model	LucentBrick is the only supported model.
Output Format	FortiGate is the only supported output format.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Set policy comment with source config line	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Output Directory	Select the folder where the output configuration is saved.

Source Configuration Selection



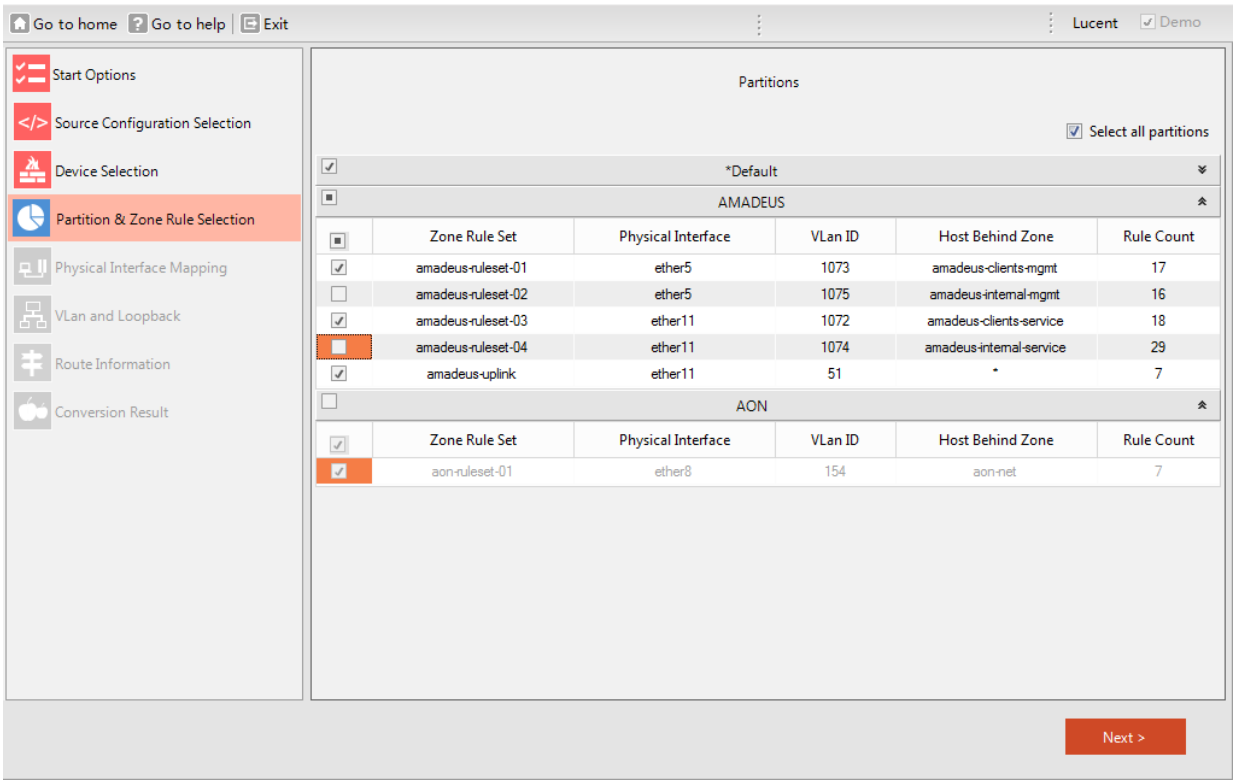
Setting	Description
Source Configuration Folder	Select the input folder.

Device Selection



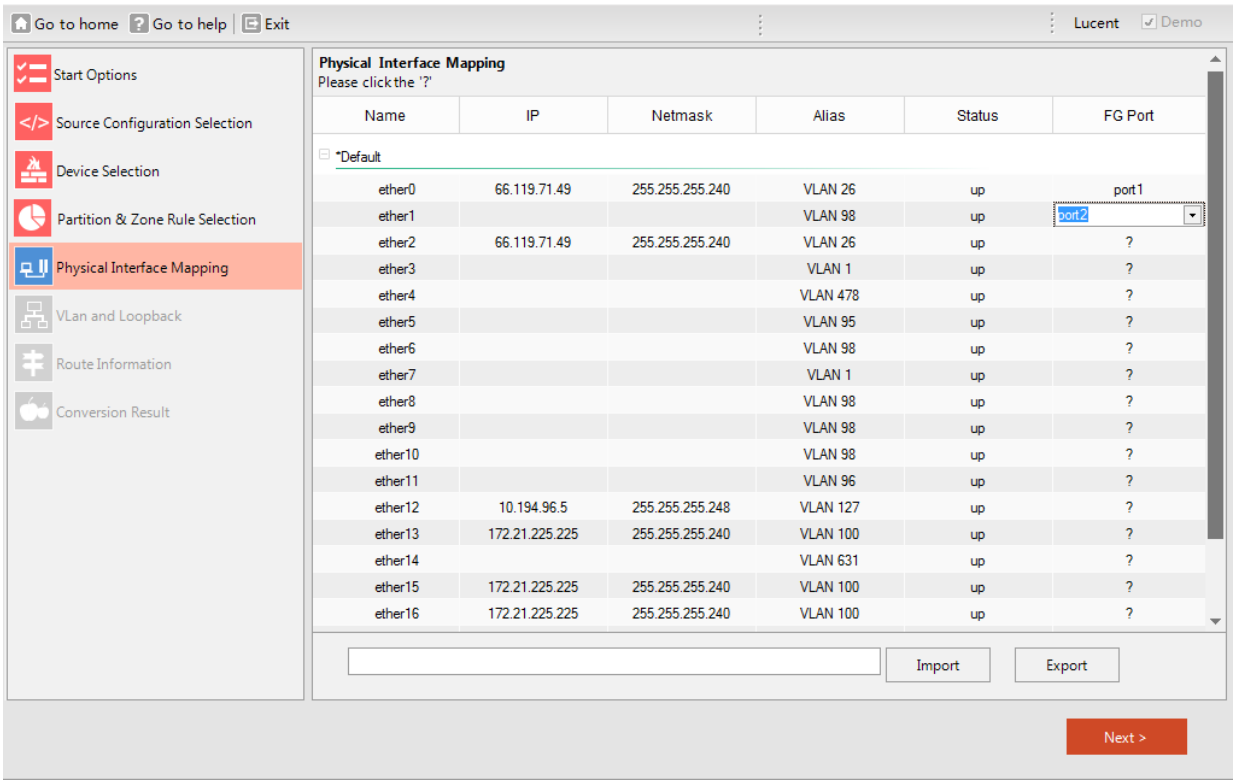
Setting	Description
Retail Branch Batch Mode	Select to specify multiple firewalls from the list. Select only firewalls with the same interfaces. For more information, see Using retail branch batch conversion mode on page 74
Device Selection	Select the firewalls to convert.

Partition & Zone Rule Selection



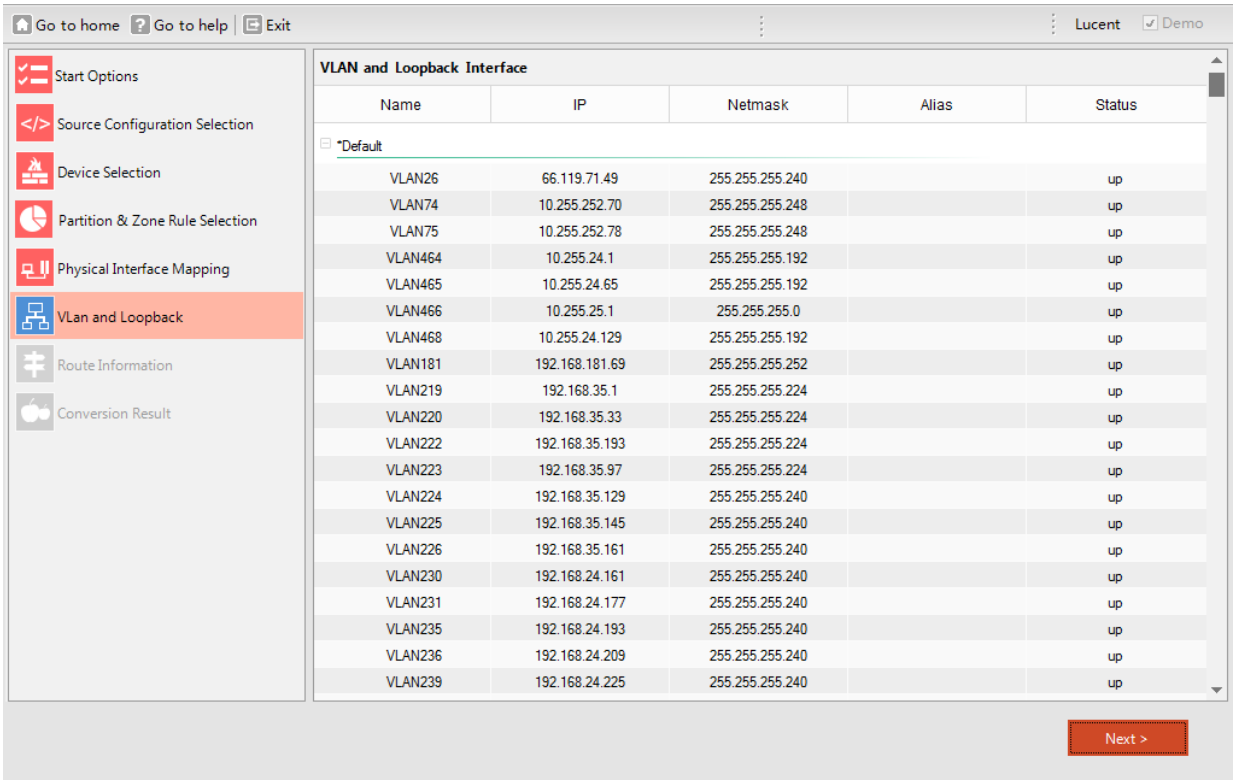
Setting	Description
Select all partitions	Select to select all partitions and clear it to de-select all partitions.
Partition selection	Use the check box to select a partition to include in the conversion. Click the pair of arrows on the right to open or close the detailed partition view, which shows the individual zone rules within a partition.
Zone rule selection	Use the check box to select a zone rule to include in the conversion.

Physical Interface Mapping



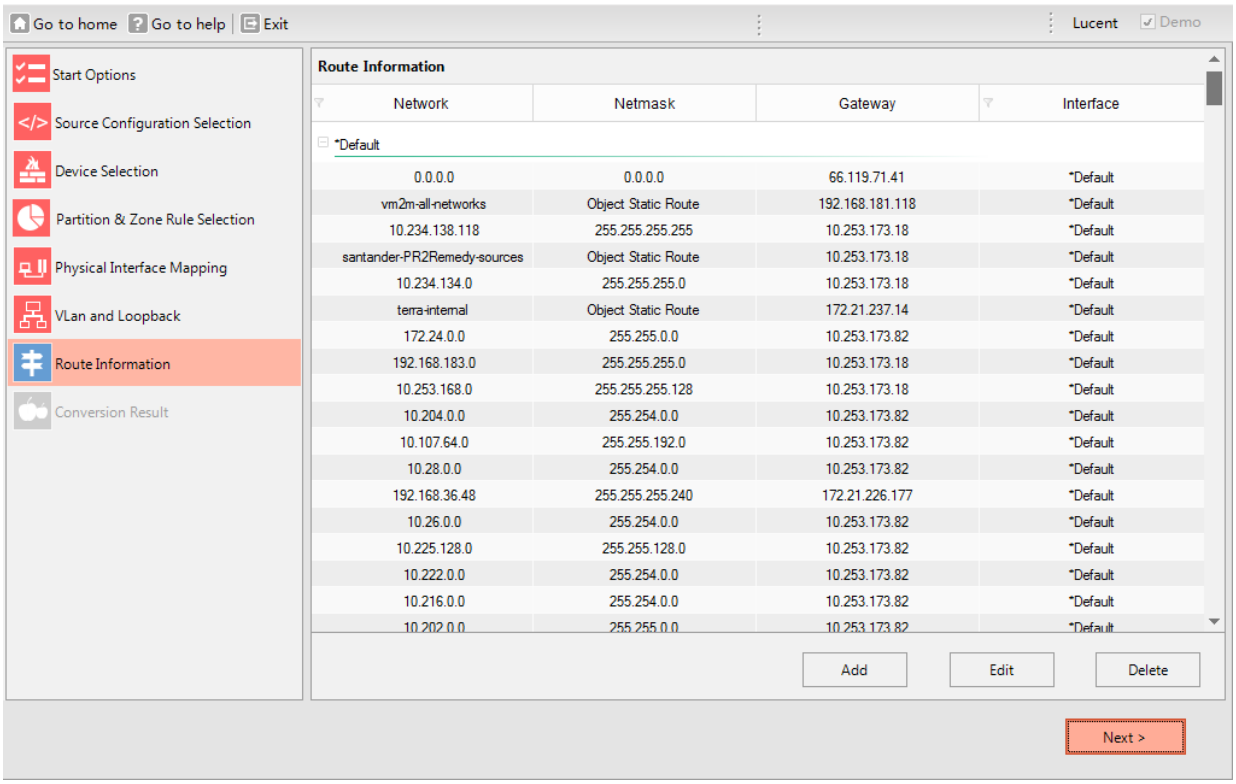
Setting	Description
FG port	Click to assign a FortiGate port for each interface.
(table column)	Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

VLAN and Loopback



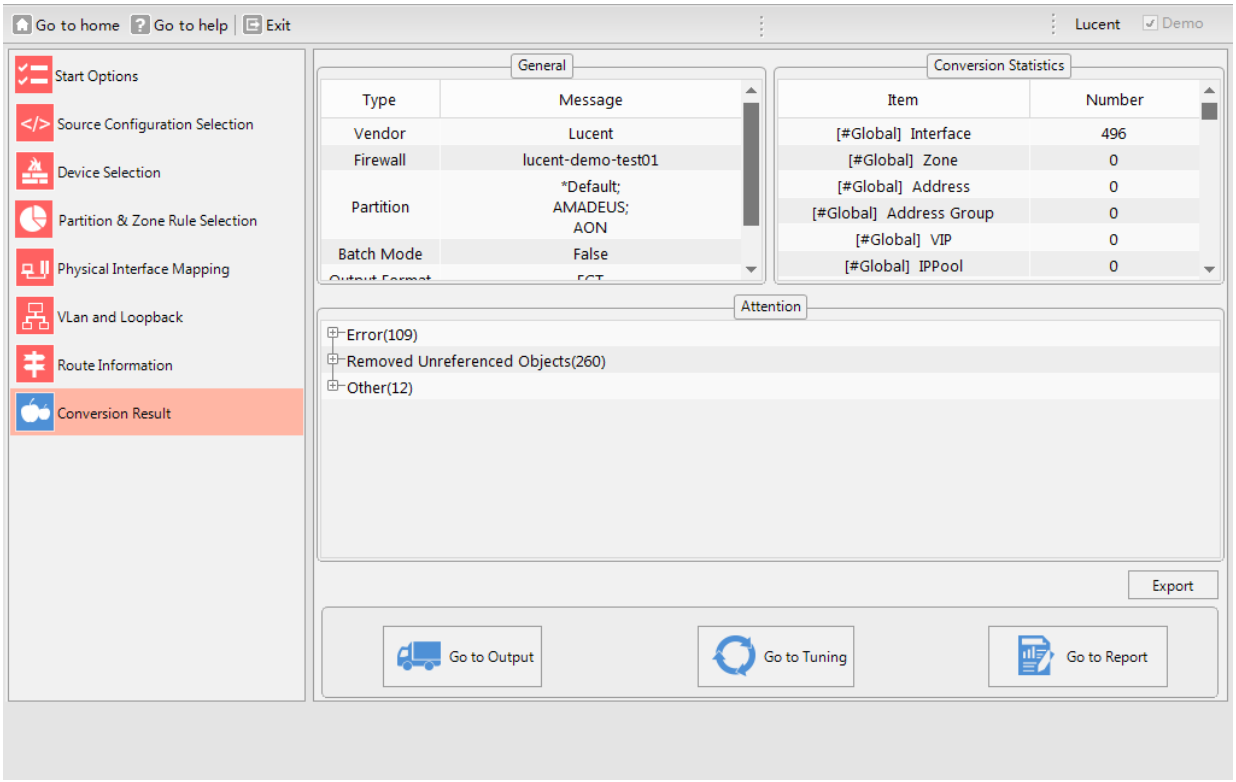
For information only. No settings.

Route Information



Setting	Description
Add	Click to add a route.
Edit	Click to edit the selected route.
Delete	Click to delete the selected route.

Conversion Result



Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81.
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see Viewing the results of your automatic conversion on page 79

Check Point conversion wizard

The pages that the Check Point conversion wizard displays depend on whether your source configuration is SmartCenter or Provider-1.

Including object comments in the output configuration

By default, output configurations from Check Point do not include:

- comments for interface, address, service, or rule objects
- review memo information for policy objects

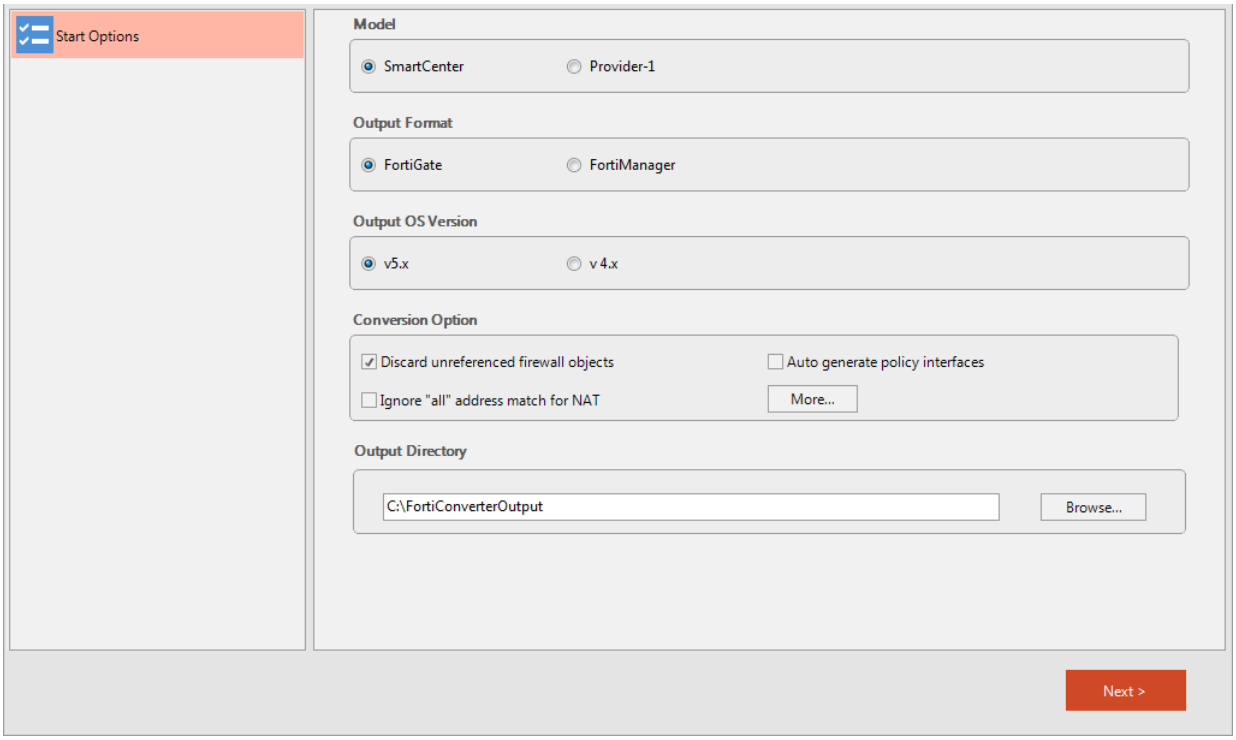
To configure FortiConverter to include object comments

1. Before you start the conversion wizard, open the file CheckpointOptions.txt in the FortiConverter installation directory in a plain-text editor. (The default location of the file is C:\Program Files (x86) \Fortinet\FortiConverter\CheckpointOptions.txt.)
2. Remove the # (number sign) from one or more of the following entries to include the corresponding data in the output configuration:

```
#interface comment
#address comment
#service comment
#rule comment
#policy review memo
```

3. Save your changes, and then start the wizard to begin the conversion process.

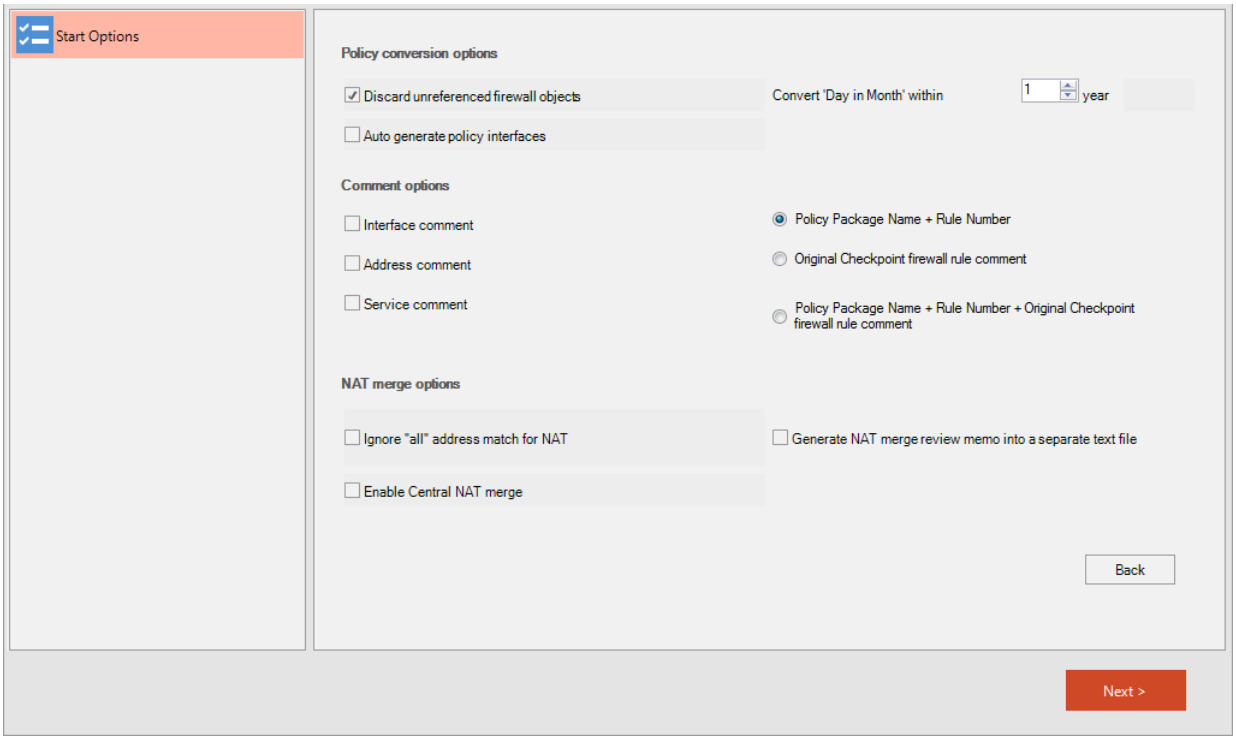
Start Options



Setting	Description
Model	Select the source Check Point model.
Output Format	Select the appropriate output for your target Fortinet device. You can convert Provider-1 to FortiManager output only.

Setting	Description
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Ignore “all” address match for NAT	Specifies whether FortiConverter ignores addresses with an “all/any” address when it merges a NAT rule and a security rule to create a FortiGate NAT policy. (In most cases, this type of address matches anything.)
Auto generate policy interfaces	Specifies whether FortiConverter generates policy interfaces using the Checkpoint route file.
More	Displays additional start options. See Start Options - More on page 30.
Output Directory	Select the folder where the output configuration is saved.

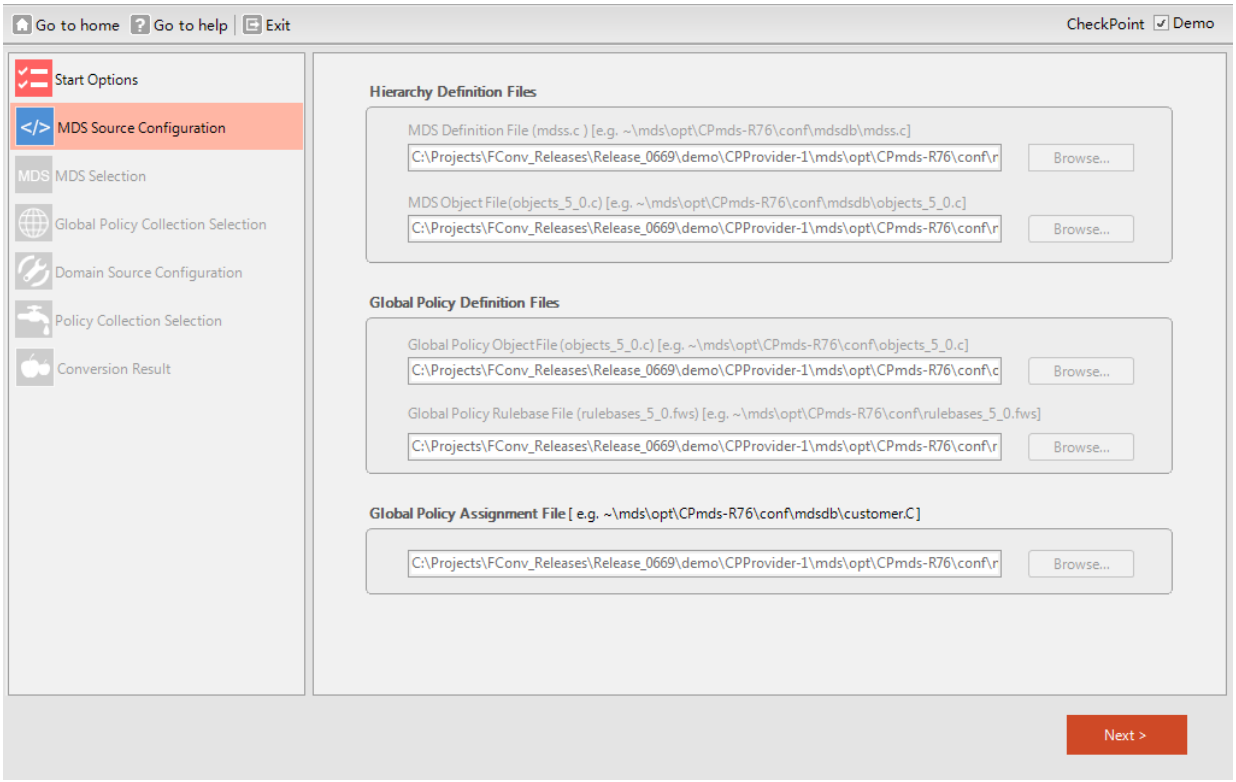
Start Options - More



Setting	Description
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.

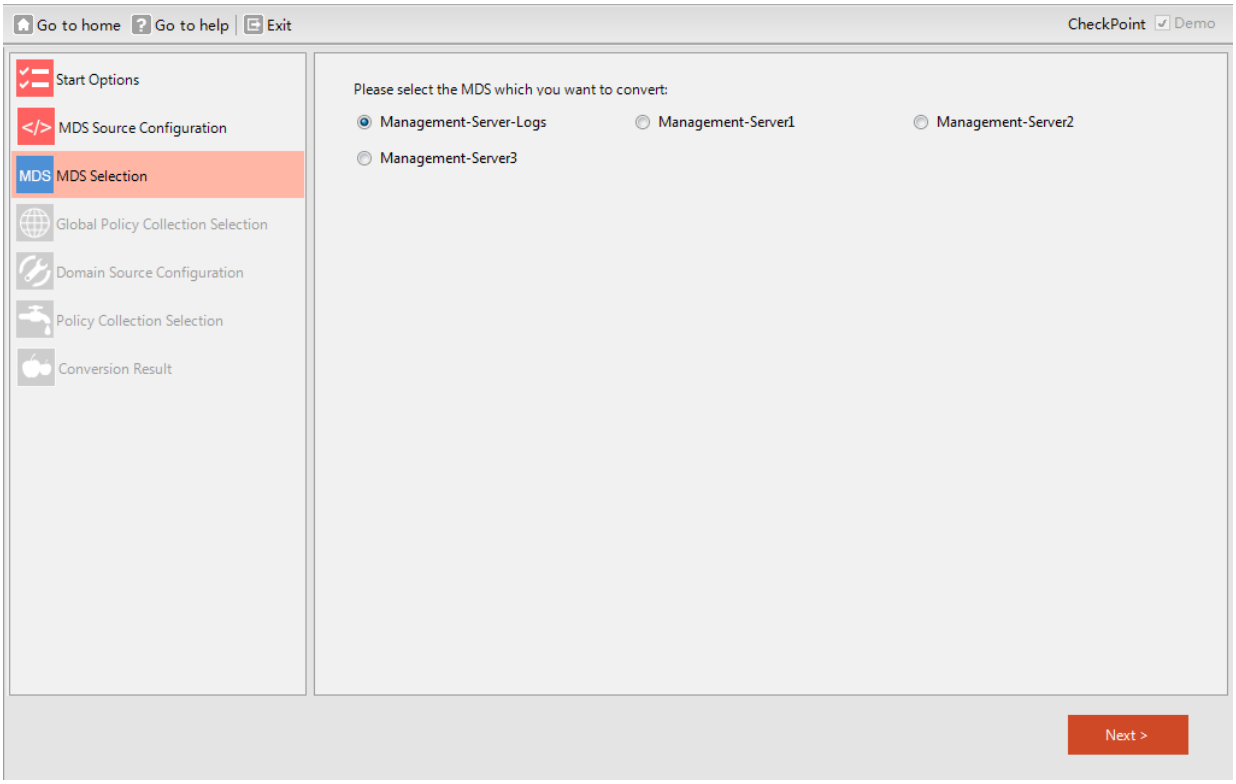
Setting	Description
Auto generate policy interfaces	Specifies whether FortiConverter generates policy interfaces using the Check Point route file.
Convert 'Day in Month' within X year	Specifies how many years of one-time schedules to generate. The wizard converts Check Point "day in month" schedules into equivalent one-time FortiGate schedules.
Interface comment	Specifies whether FortiConverter copies the interface comment from the source configuration to the mapped FortiGate interface.
Address comment	Specifies whether FortiConverter copies the address comment from source configuration to the converted FortiGate address.
Service comment	Specifies whether FortiConverter copies the service comment from the source configuration to converted FortiGate service.
Policy Package Name + Rule Number **Original Check Point firewall rule comment** **Policy Package + Rule Number + Original Check Point firewall rule comment**	Specifies what information FortiConverter includes in the converted policy comment.
Ignore "all" address match for NAT	Specifies whether FortiConverter ignores addresses with an "all/any" address when it merges a NAT rule and a security rule to create a FortiGate NAT policy. (In most cases, this type of address matches anything.)
Enable Central NAT merge	Specifies whether FortiConverter converts Hide NATs to FortiGate central NATs instead of a policy-based NATs.
Generate NAT merge review memo as a separate text file	Specifies whether FortiConverter generates a separate text file for NAT merge policies. FortiConverter generates NAT merge policies by merging NAT and security rules in the source configuration.
Back	Displays the main Start Options page.

MDS Source Configuration (Provider-1 only)



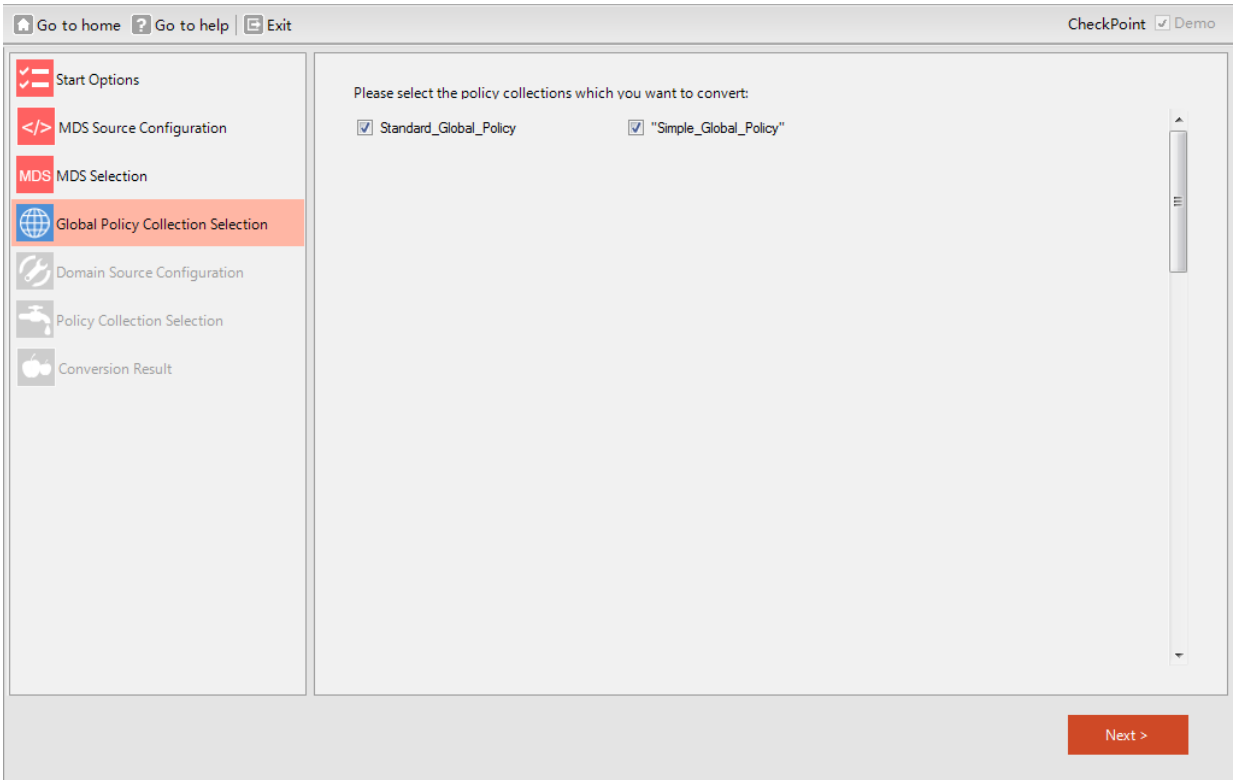
Setting	Description
Browse	Select the Provider-1 configuration files.

MDS Selection (Provider-1 only)



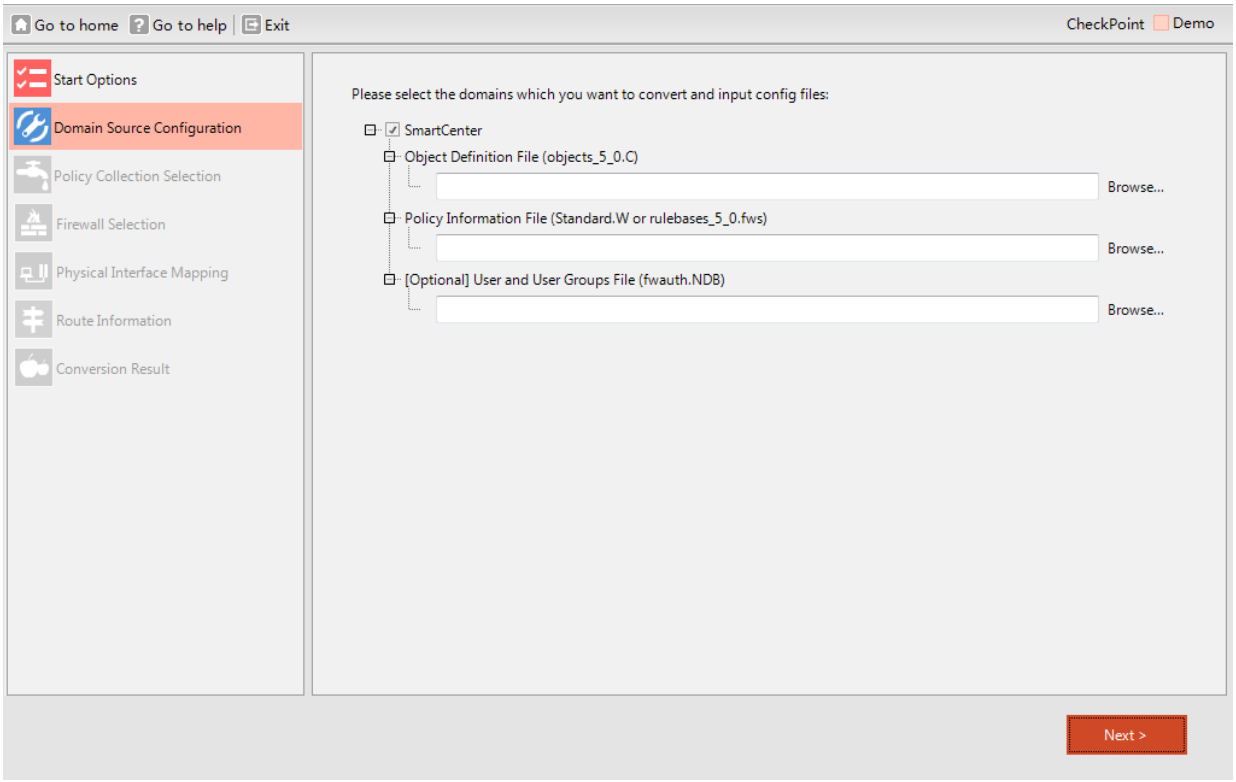
Setting	Description
Please select the MDS which you want to convert	Select the domain to convert.

Global Policy Collection Selection (Provider-1)



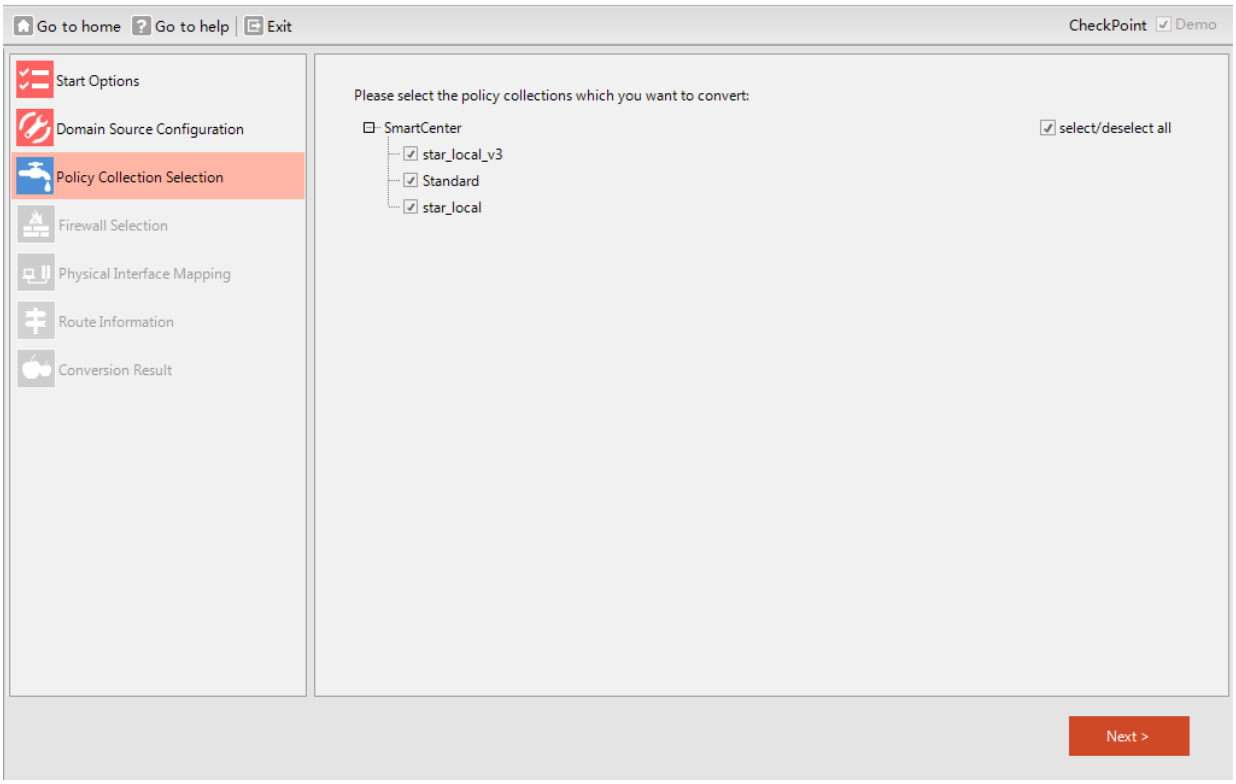
Setting	Description
Standard_Global_Policy	Specifies whether FortiConverter converts the Standard Global Policy. You can select both **Standard Global Policy** and **Simple Global Policy**.
Simple_Global_Policy	Specifies whether FortiConverter converts the Simple Global Policy.

Domain Source Configuration



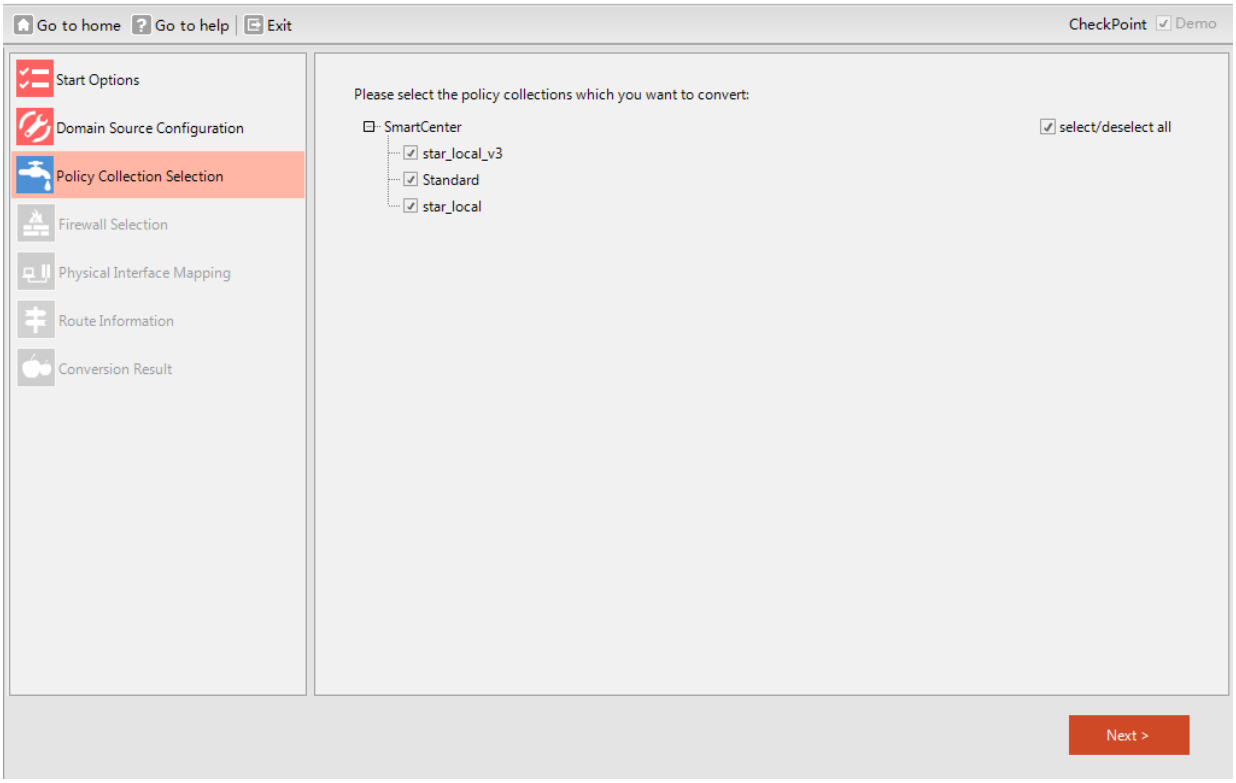
Setting	Description
Browse	Click to select domain source configuration files. For information on acquiring these files, see Downloading the source configuration files on page 17.

Policy Collection Selection



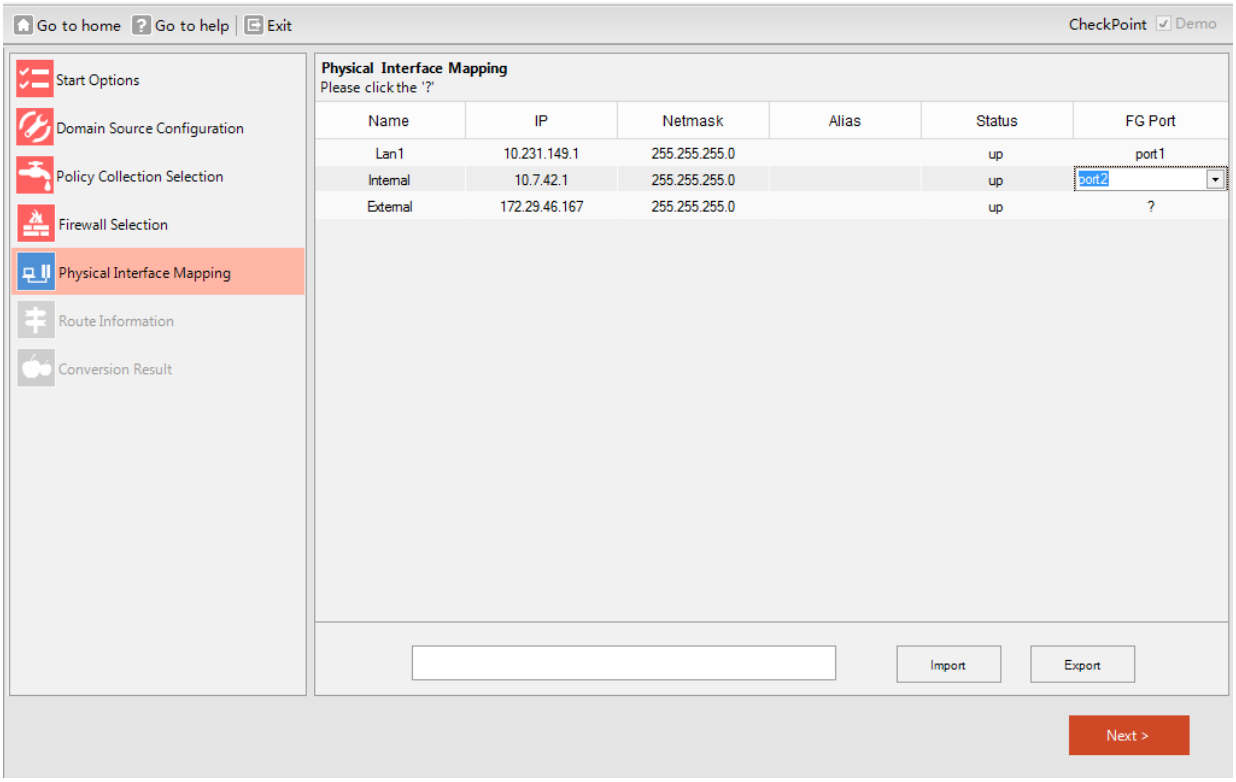
Setting	Description
(policy collection item)	Select the policy collections to convert.
Select/deselect all	Select or clear all policy collection items.

Firewall Selection (SmartCenter only)



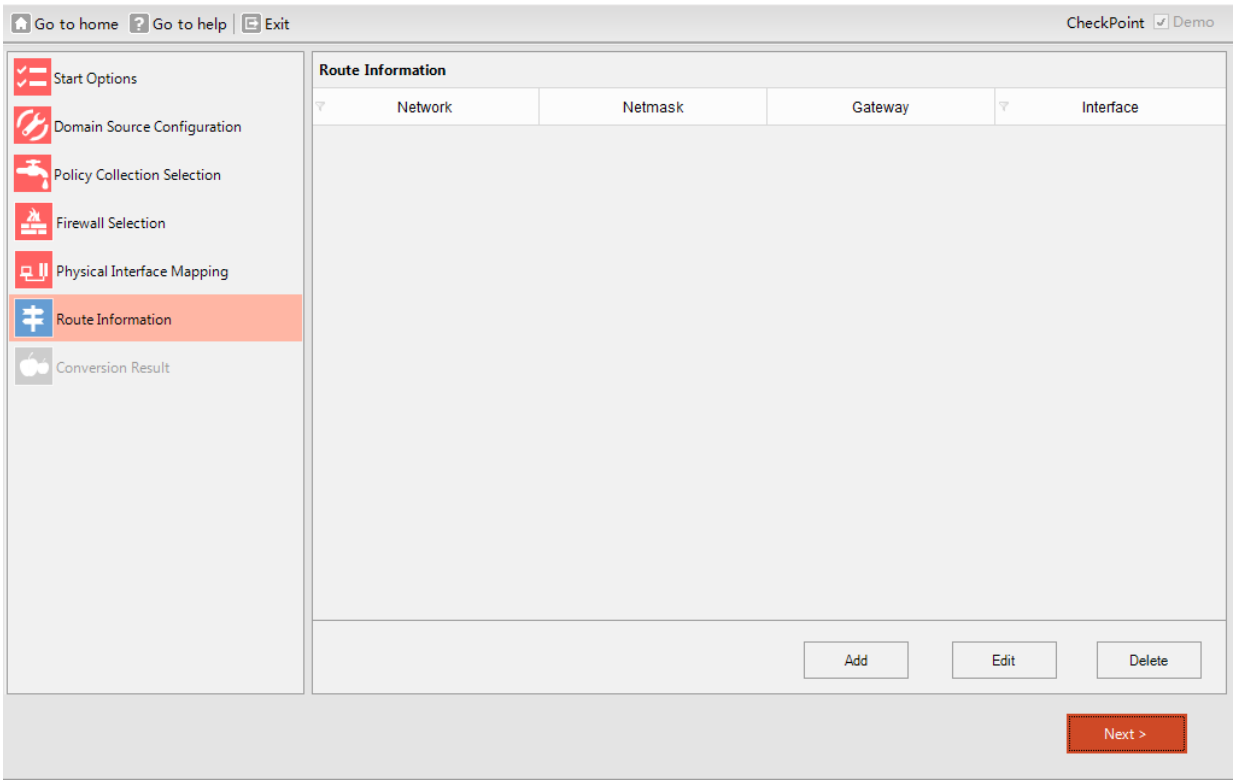
Setting	Description
Retail Branch Batch Mode	Select to specify multiple firewalls from the list. Select only firewalls with the same interfaces. For more information, see Using retail branch batch conversion mode on page 74
(firewall item)	Select one or more firewalls to convert.
Route File	(Optional) Enter the path and file name of a file that contains route information, or click **Browse** to select it.

Physical Interface Mapping (SmartCenter only)



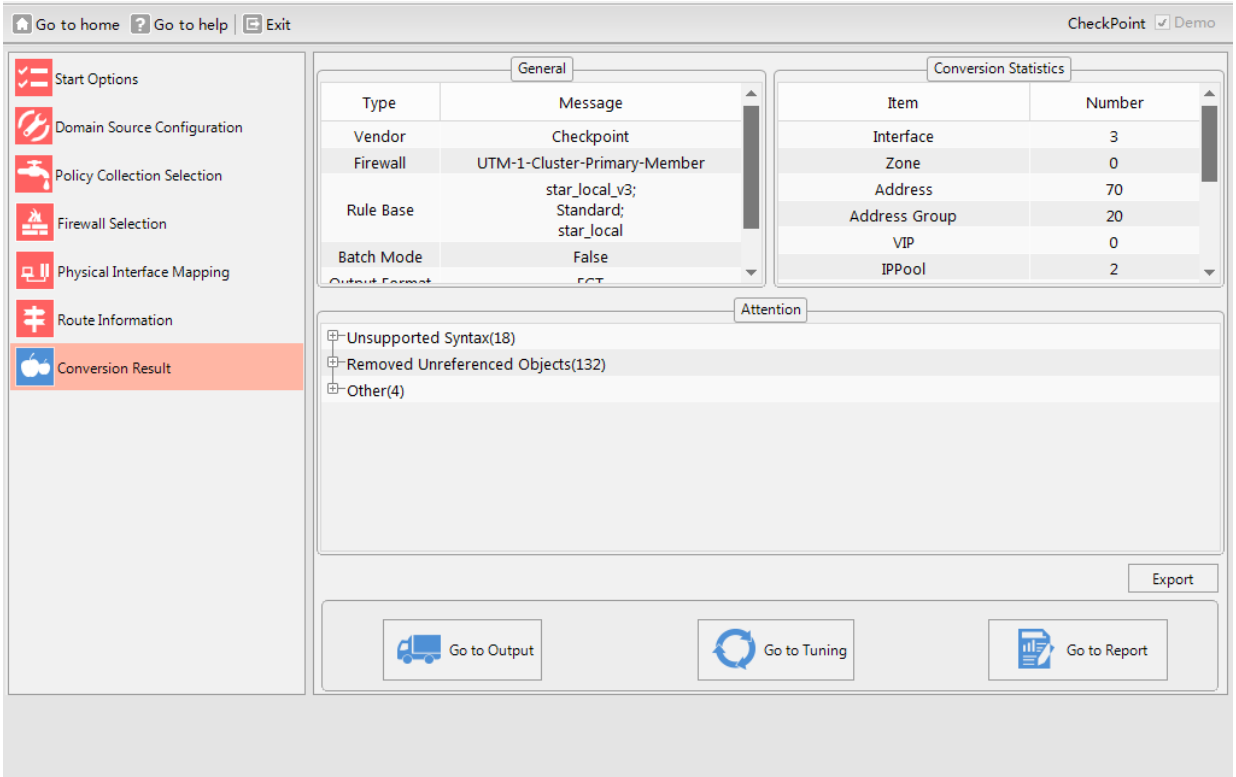
Setting	Description
FG port	Click to assign a FortiGate port for each interface.
(table column)	Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

Route Information (SmartCenter only)



Setting	Description
Add	Click to add a route.
Edit	Click to edit the selected route.
Delete	Click to delete the selected route.

Conversion Result

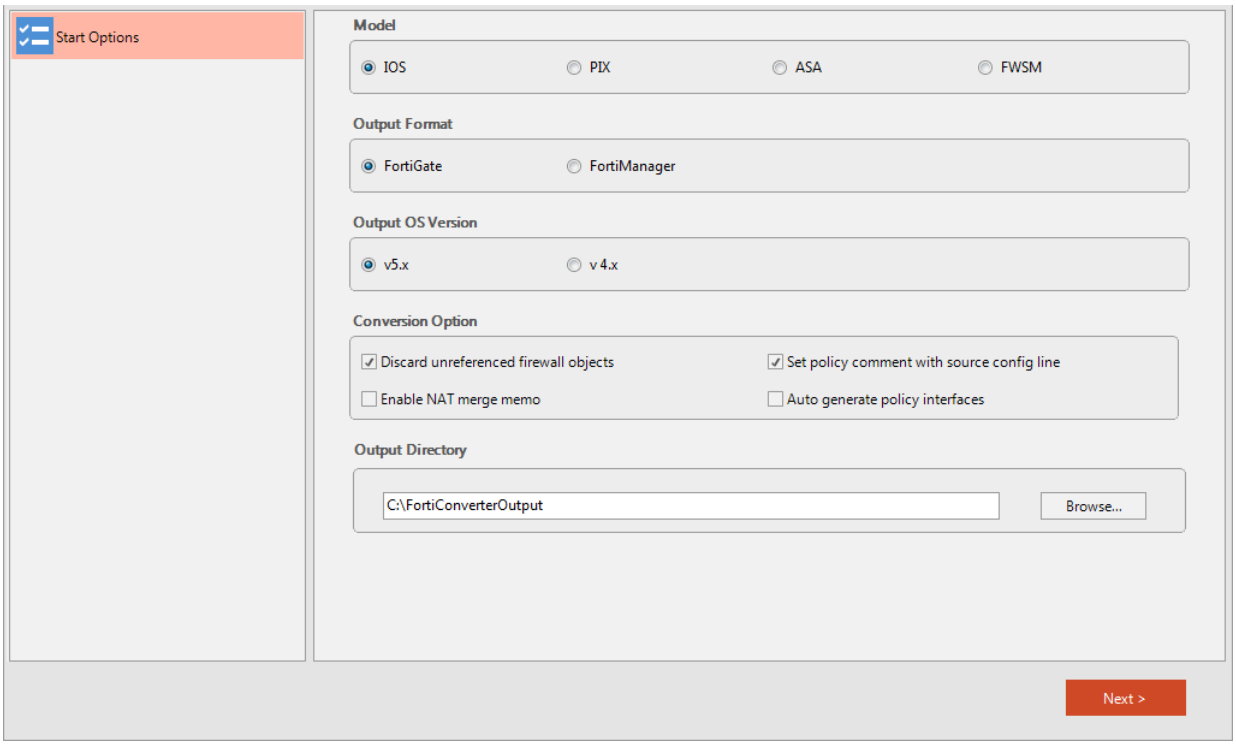


Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81.
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see Viewing the results of your automatic conversion on page 79

Cisco conversion wizard

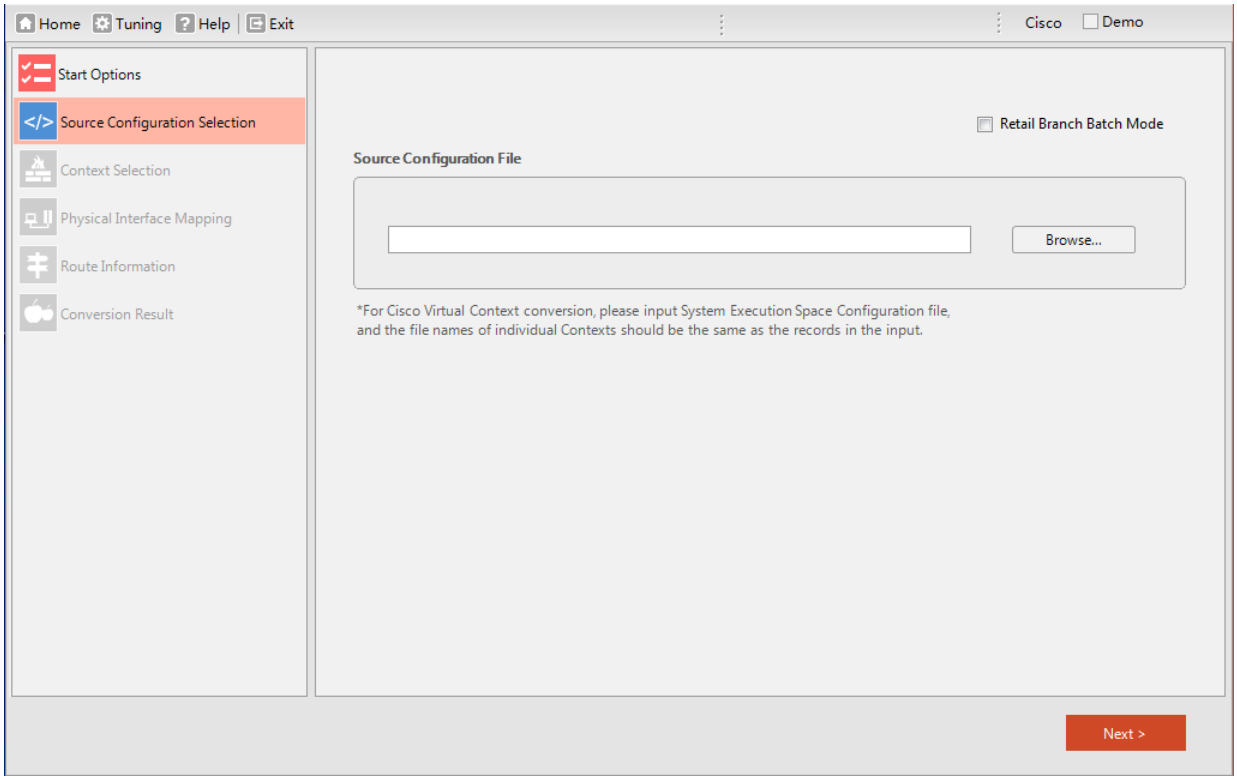
Start Options



Setting	Description
Model	Select the model of the source configuration.
Output Format	Select the appropriate output format for your FortiGate device.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Enable NAT merge memo	Specifies whetherFortiConverter copies NAT merge policies to a separate text file that you can review. The file name is `PolicyMemo.txt`.
Set policy comment with source config line	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Auto generate policy interfaces	Specifies whether FortiConverter generates policy interfaces using the Cisco route file.

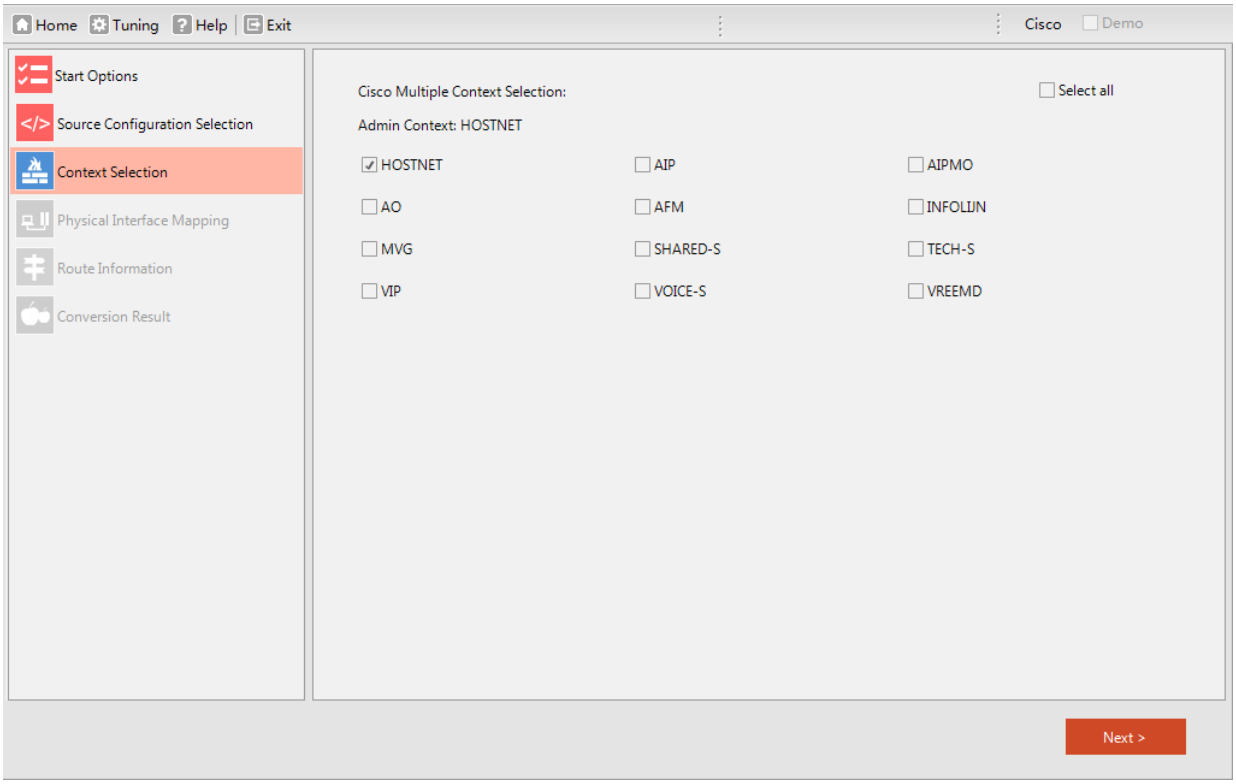
Setting	Description
Output Directory	Select the folder where the output configuration is saved.

Source Configuration Selection



Setting	Description
Retail Branch Batch Mode	Select to specify multiple source configuration files. Ensure that all the source files use the same interface. For more information, see Using retail branch batch conversion mode on page 74
Source Configuration File	Select the input file or files.

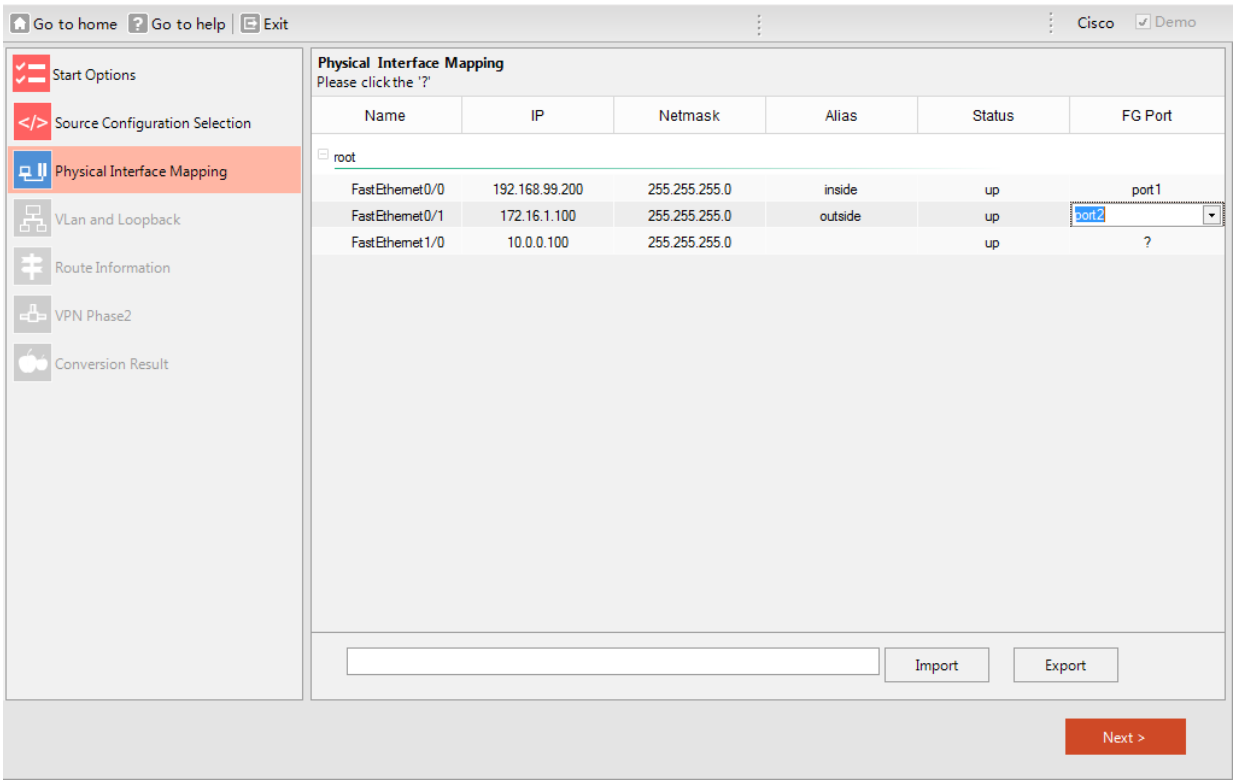
Context Selection



Select one or more virtual contexts to convert to equivalent VDOMs.

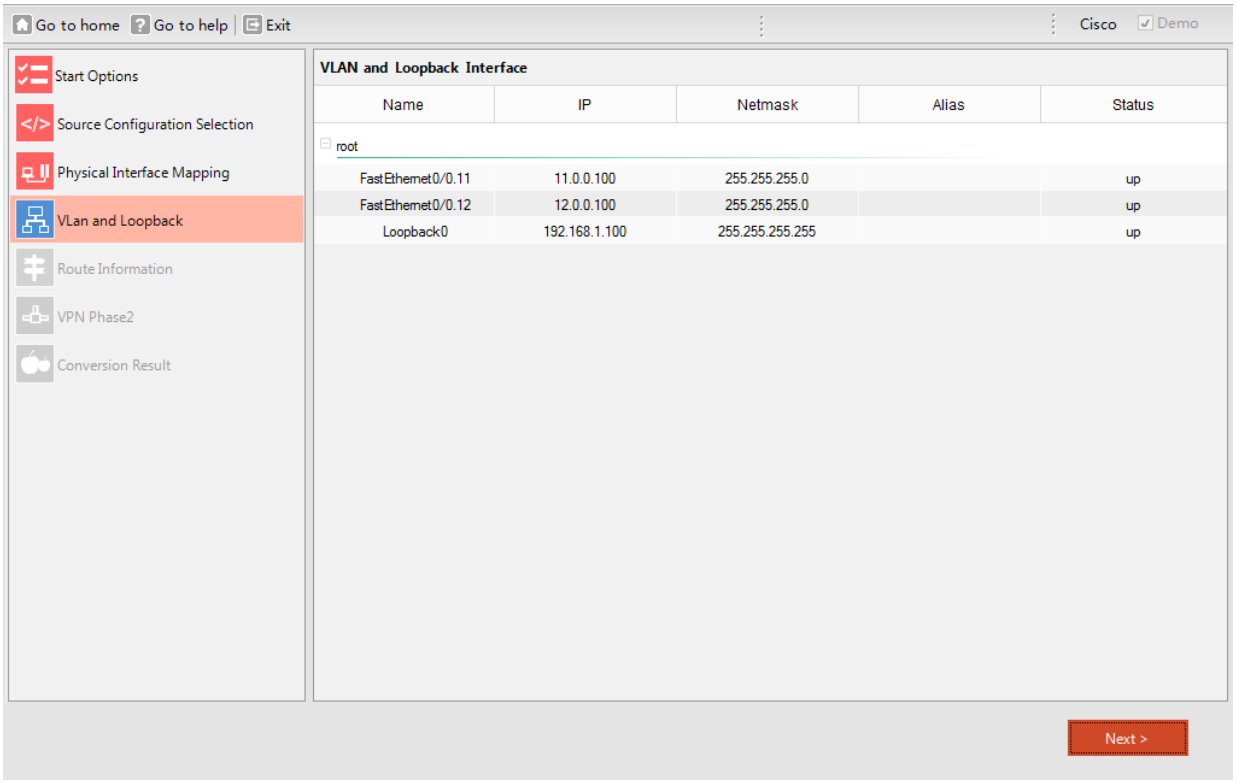
This page is displayed only if you have provided a virtual context input file.

Physical Interface Mapping



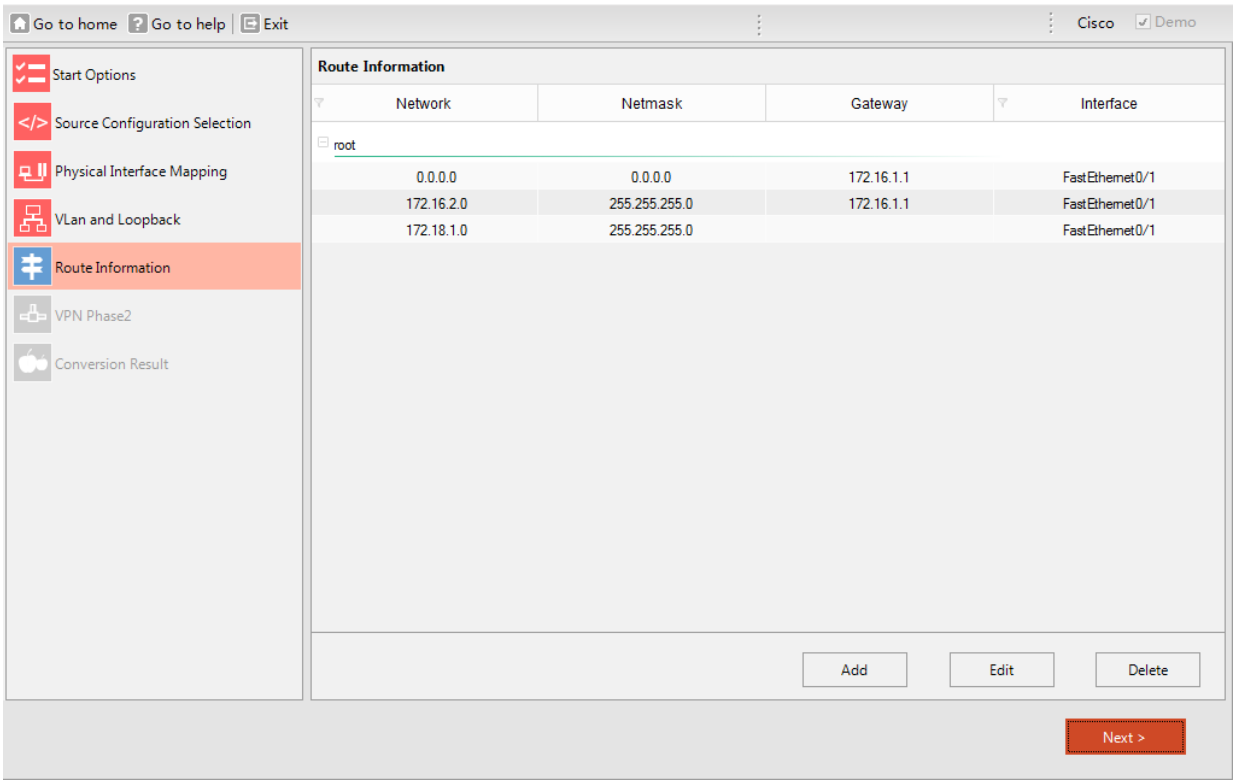
Setting	Description
FG port (table column)	Click to assign a FortiGate port for each interface. Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

VLAN and Loopback



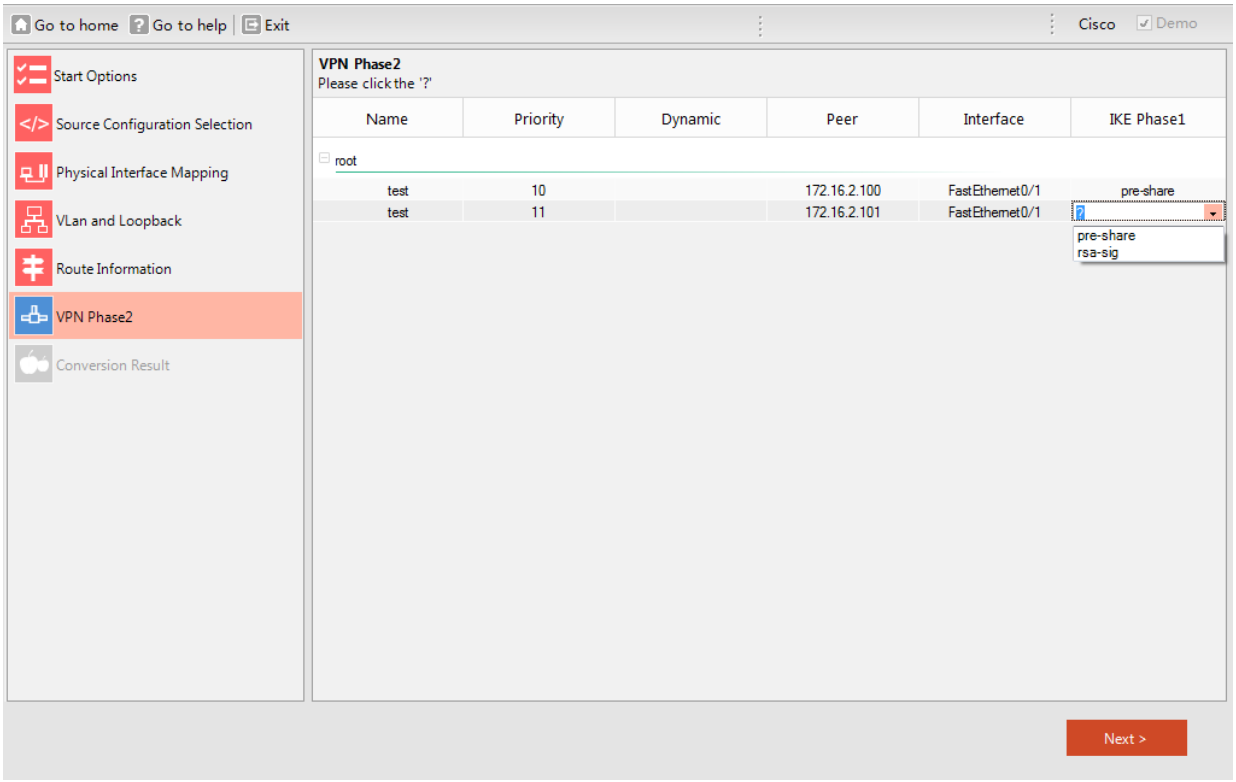
For information only. No settings.

Route Information



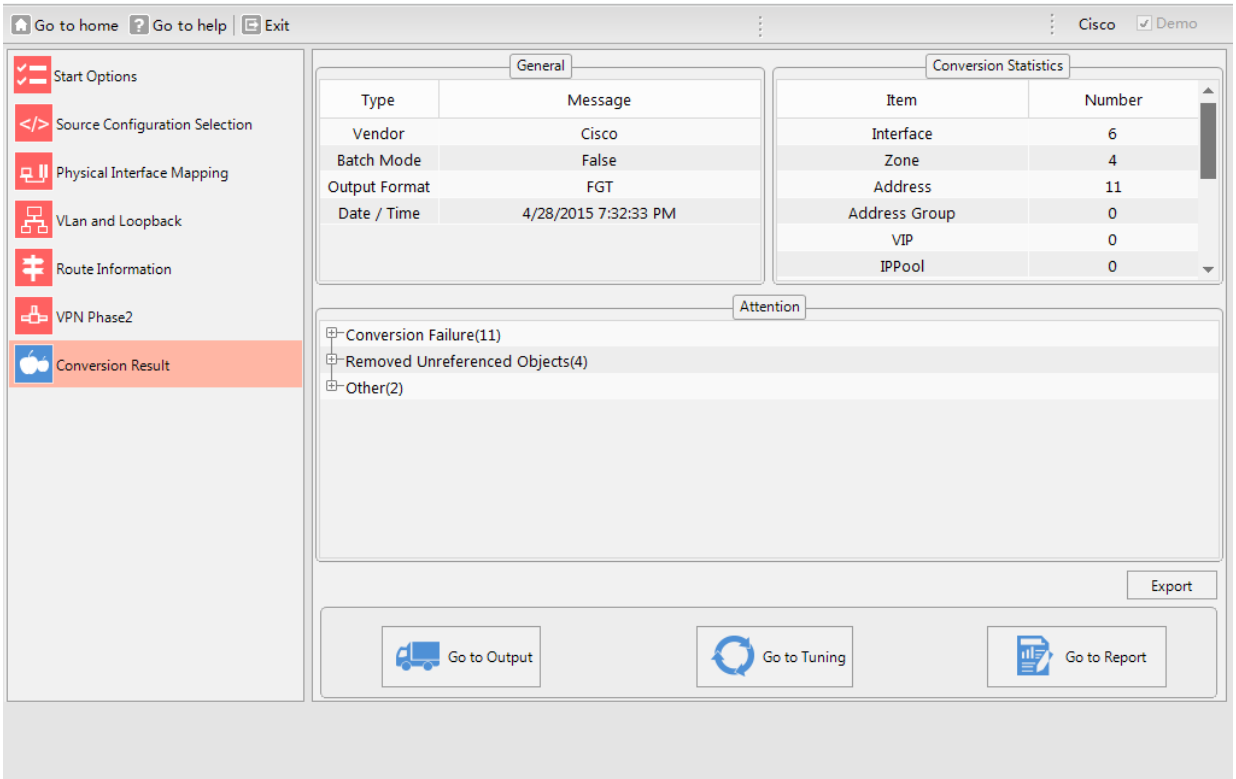
Setting	Description
Add	Click to add a route.
Edit	Click to edit the selected route.
Delete	Click to delete the selected route.

VPN Phase2



Setting	Description
IKE Phase1 (table column)	Select an IKE Phase1 authentication method: **pre-share** (preshared keys) or **rsa-sig** (RSA signatures).

Conversion Result

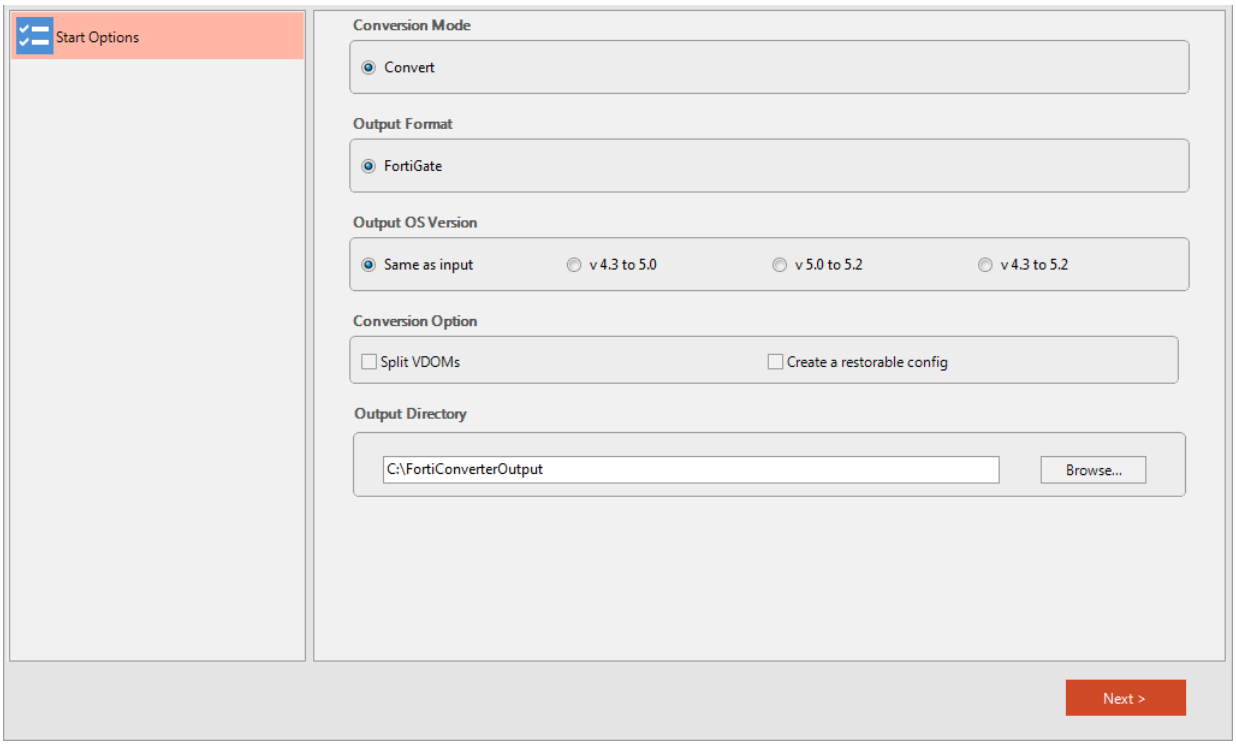


Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81.
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see Viewing the results of your automatic conversion on page 79

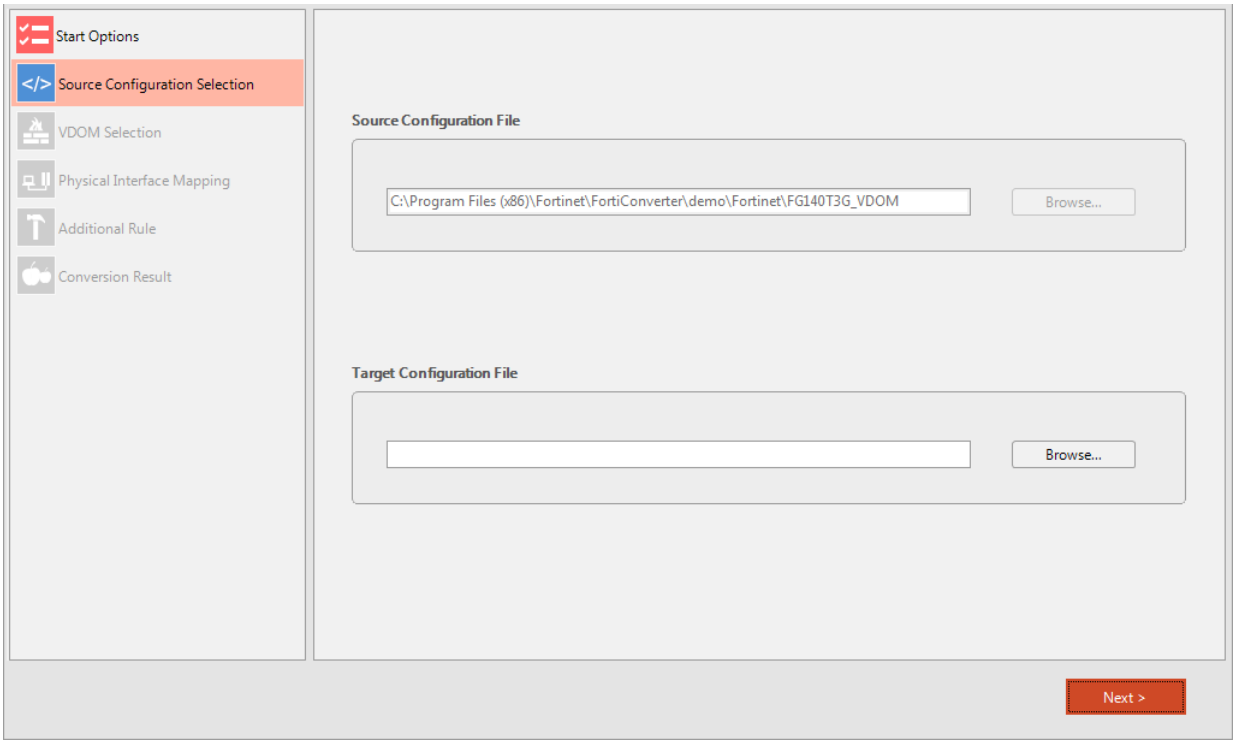
Fortinet conversion wizard

Start Options



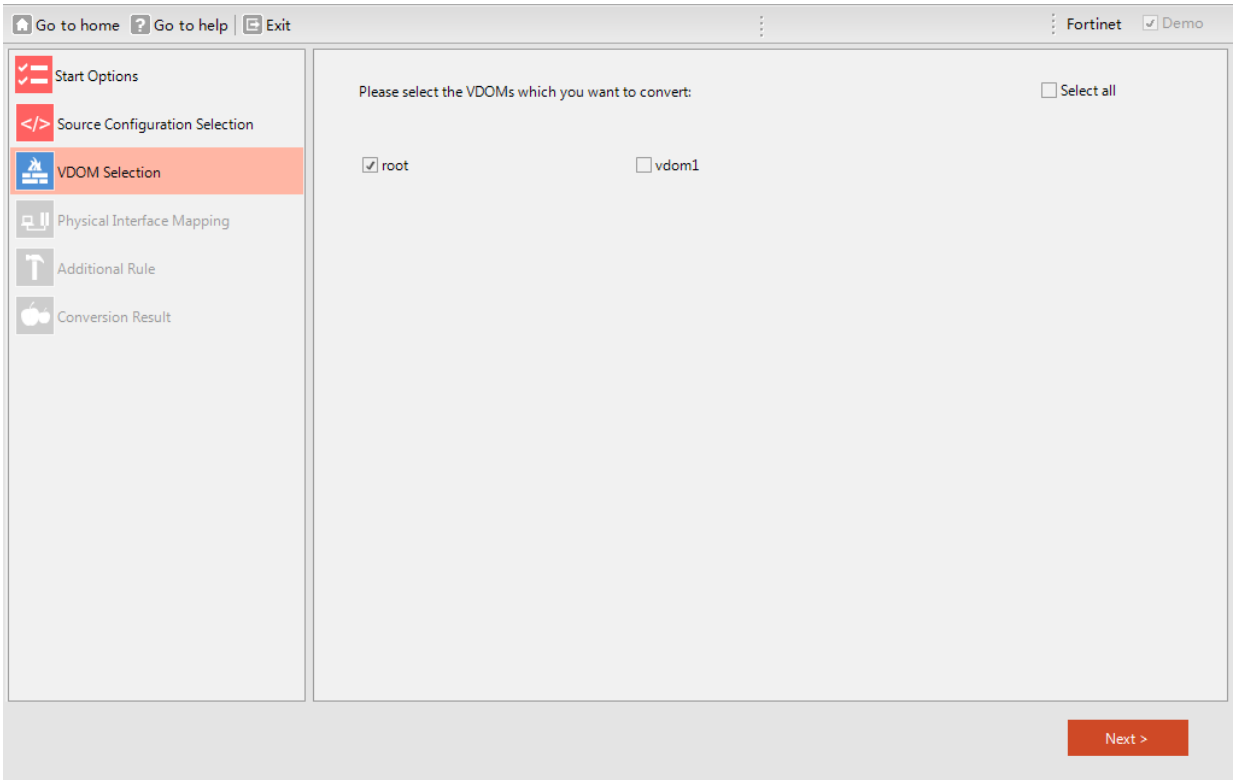
Setting	Description
Conversion Mode	Convert is the only supported task.
Output Format	FortiGate is the only supported output format.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the option that matches the OS to convert to.
Split VDOMs	Create an output configuration for each VDOM.
Create a restorable config	Specify whether FortiConverter generates configuration files that you can restore to the target device directly.
Output Directory	Select the folder where the output configuration is saved.

Source Configuration Selection



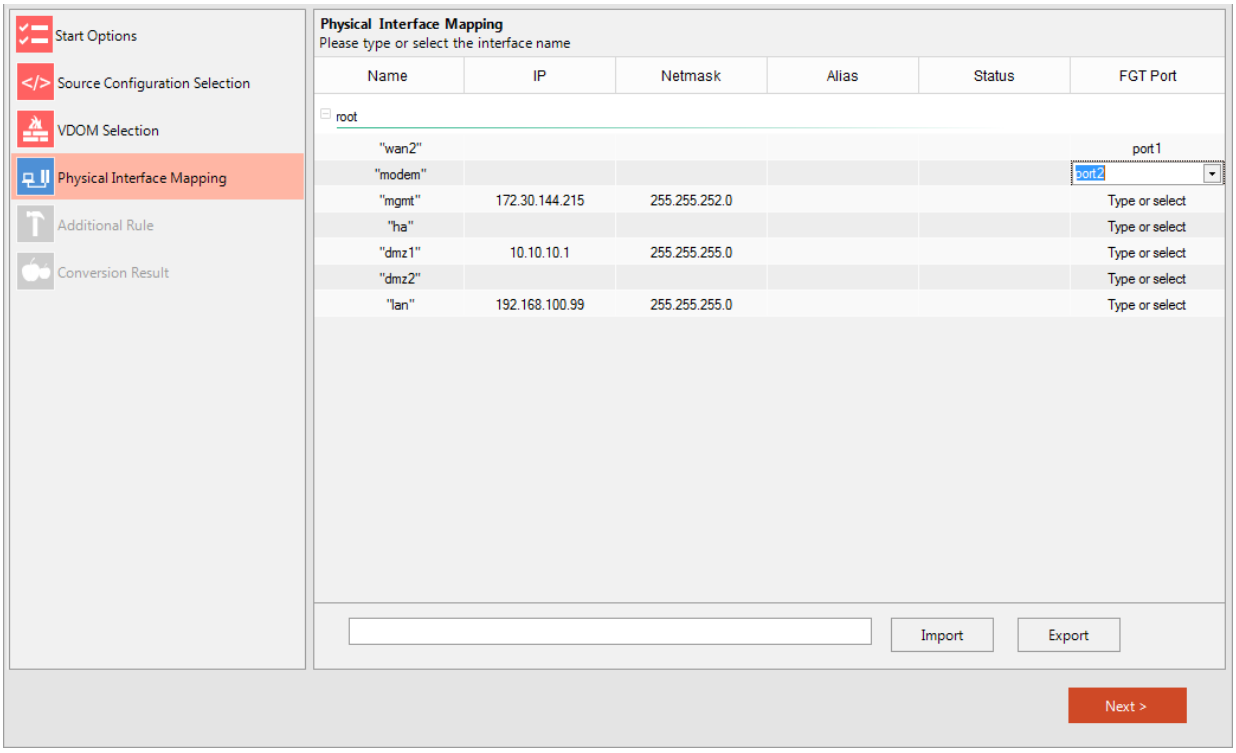
Setting	Description
Source Configuration Folder	Select the input folder.
Target Configuration File	Select the target device's default configuration. This is the device configuration before you perform any configuration tasks or after you restore the factory defaults.

VDOM Selection



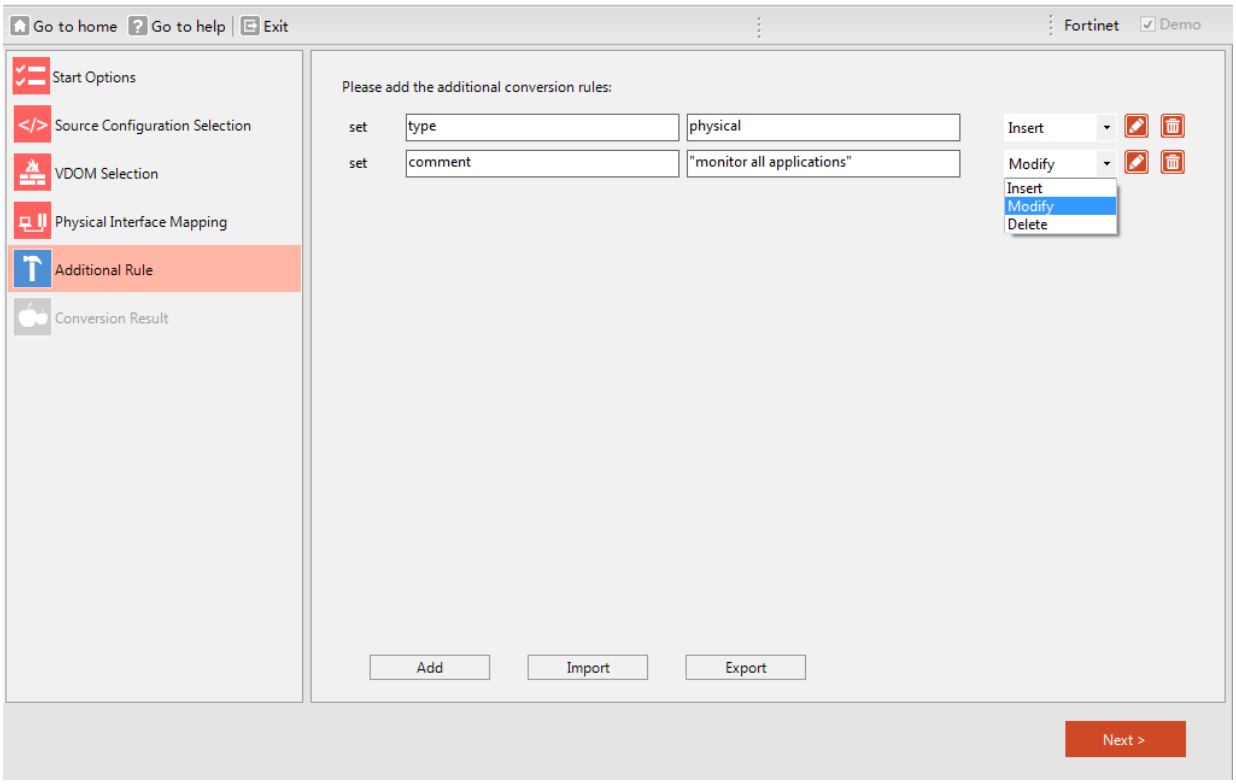
Setting	Description
Select all	Select to select all VDOMs for conversion.
(VDOM item)	Select one or more VDOMs to convert.

Physical Interface Mapping



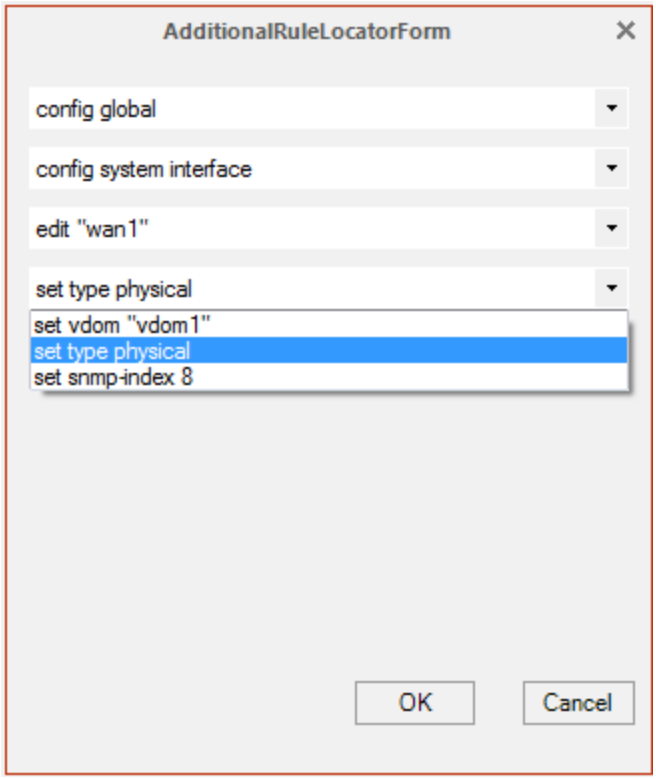
Setting	Description
FG port	Click to assign a FortiGate port for each interface.
(table column)	Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

Additional Rule

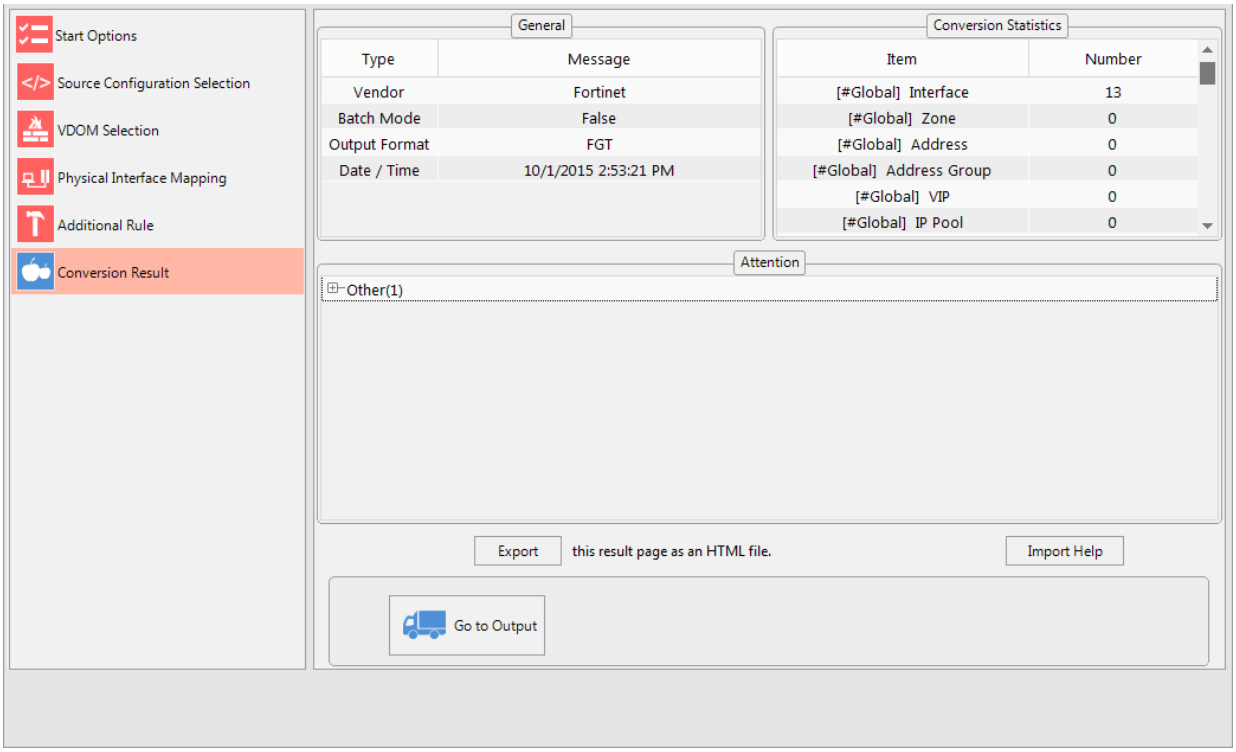


Setting	Description
Add	Click to open a dialog box that allows you to select rules from the source configuration to add. See the illustration "Additional rule locator window".
Import	Click to load a set of rule changes from a text file.
Export	Saves the current set of rule changes to a text file.
(rule table)	• Property (first field) – The property of the rule. You can edit this value. • Value (second field) – The property's value. You can edit this value. • Action (list) – Select either **Insert** (adds the rule to existing rules), **Modify** (to change the rule), or **Delete**. • Edit (pencil icon) – Opens the additional rule locator dialog box. • Delete (trash can icon) – Removes the rule from the list.

Additional rule locator dialog box



Conversion Result



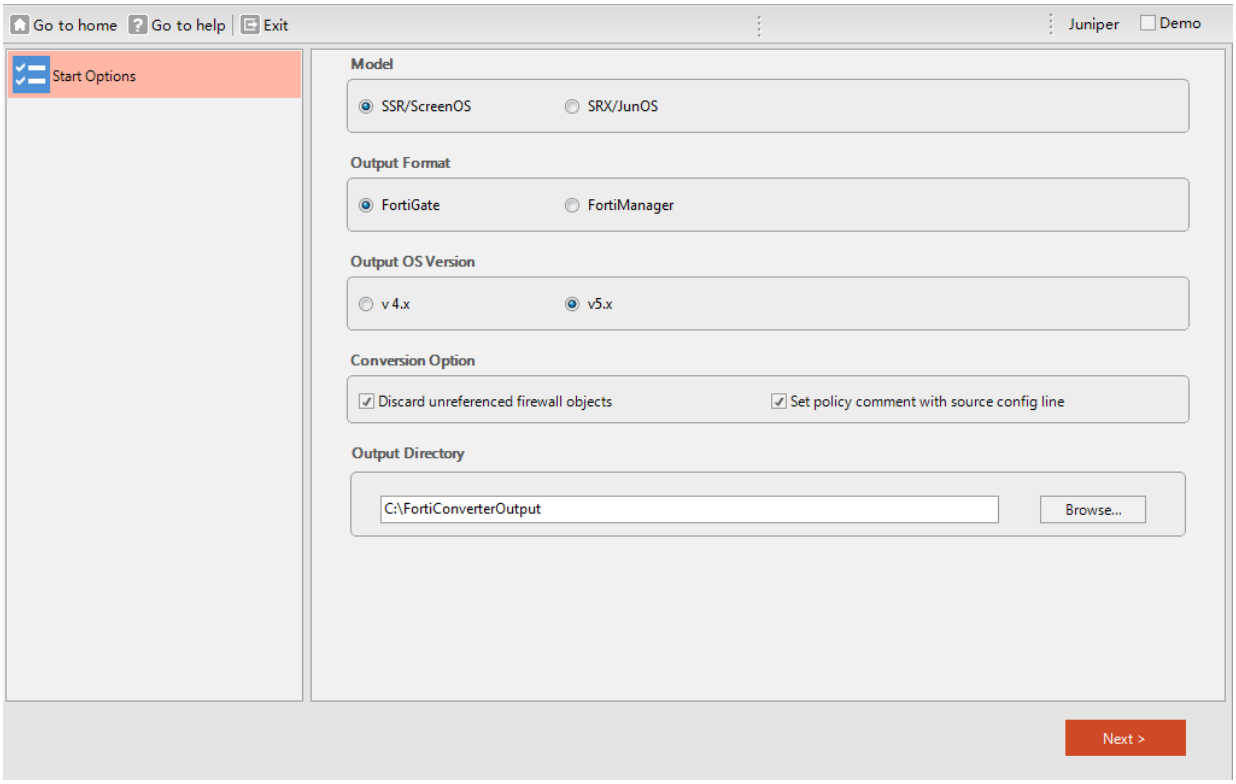
Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .

For more information, see Viewing the results of your automatic conversion on page 79

Juniper conversion wizard

By default, output configurations from Juniper do not include some configuration information, including address and service comments. For an example of how to include this information in the output, see Including object comments in the output configuration on page 28.

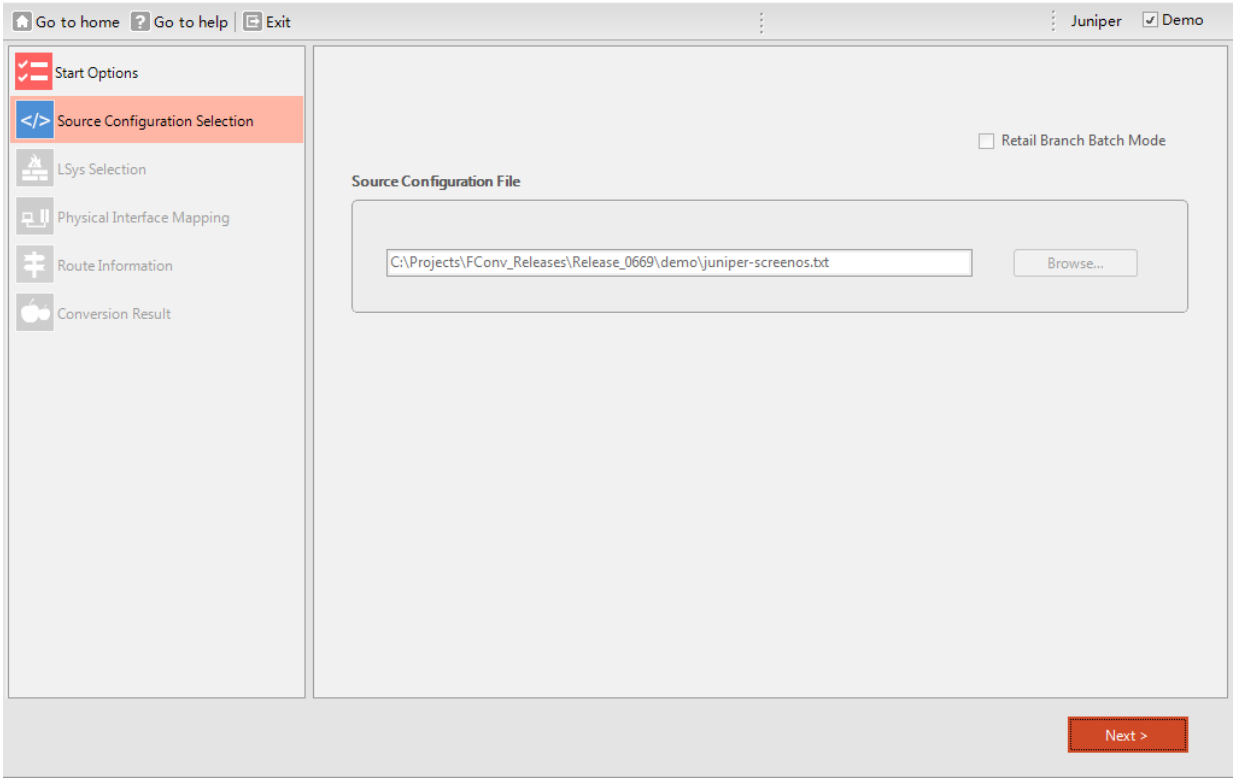
Start Options



Setting	Description
Model	Select the model of the source configuration.
Output Format	Select the appropriate output format for your FortiGate device.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.

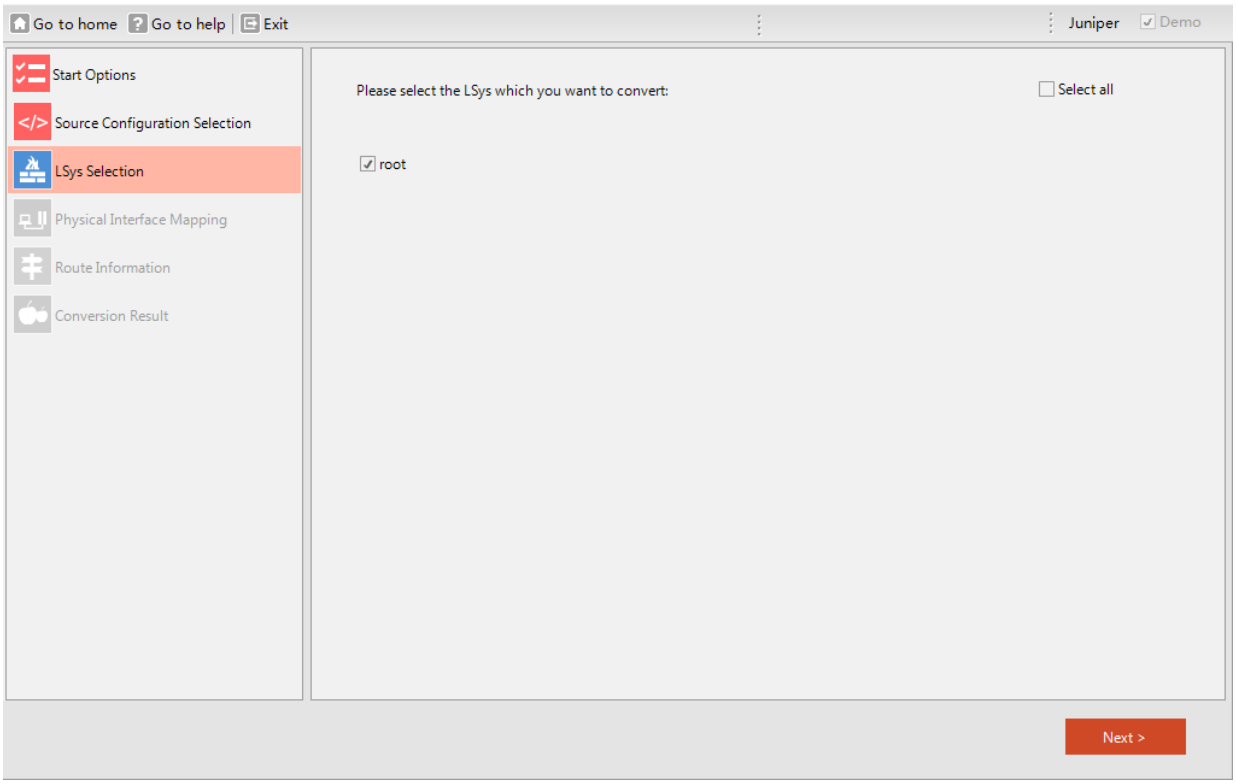
Setting	Description
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Set policy comment with source config line	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Output Directory	Select the folder where the output configuration is saved.

Source Configuration Selection



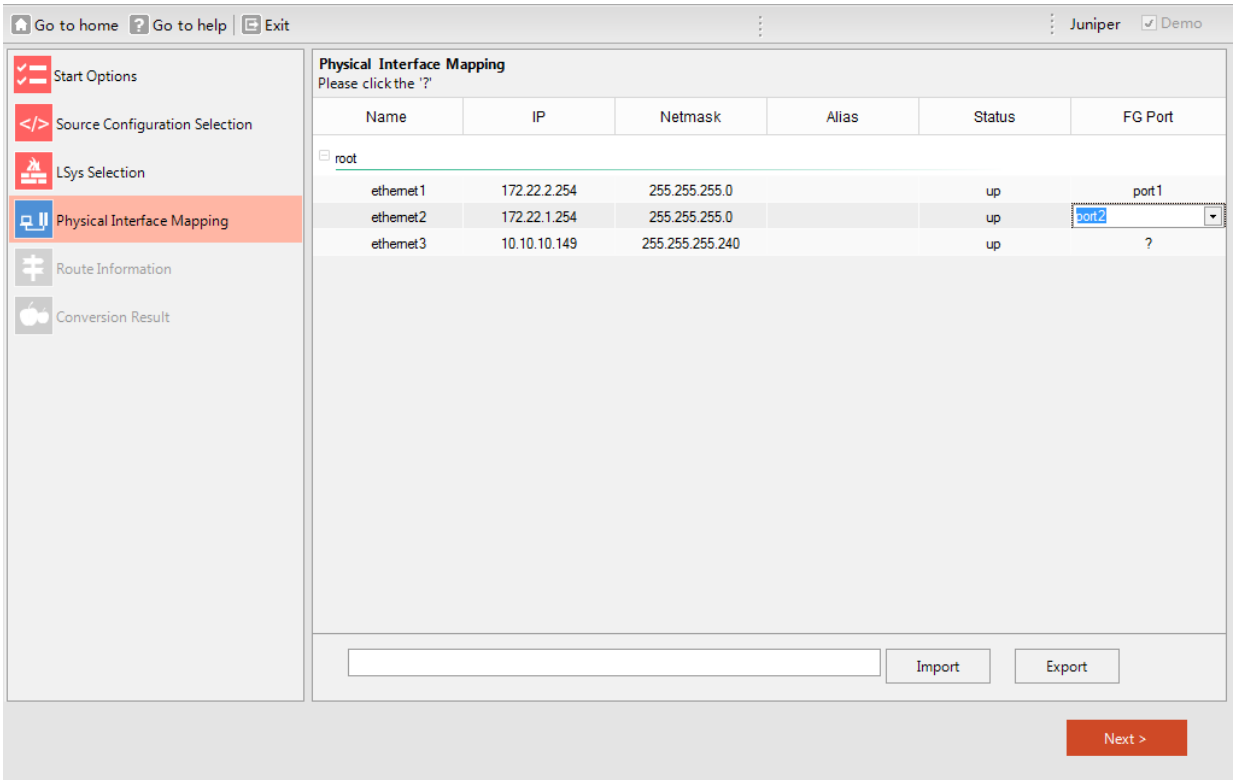
Setting	Description
Retail Branch Batch Mode	Select to specify multiple source configuration files. Ensure that all the source files use the same interface. For more information, see Using retail branch batch conversion mode on page 74
Source Configuration File	Select the input file or files.

LSYS (Junos OS) or VSYS (ScreenOS) Selection



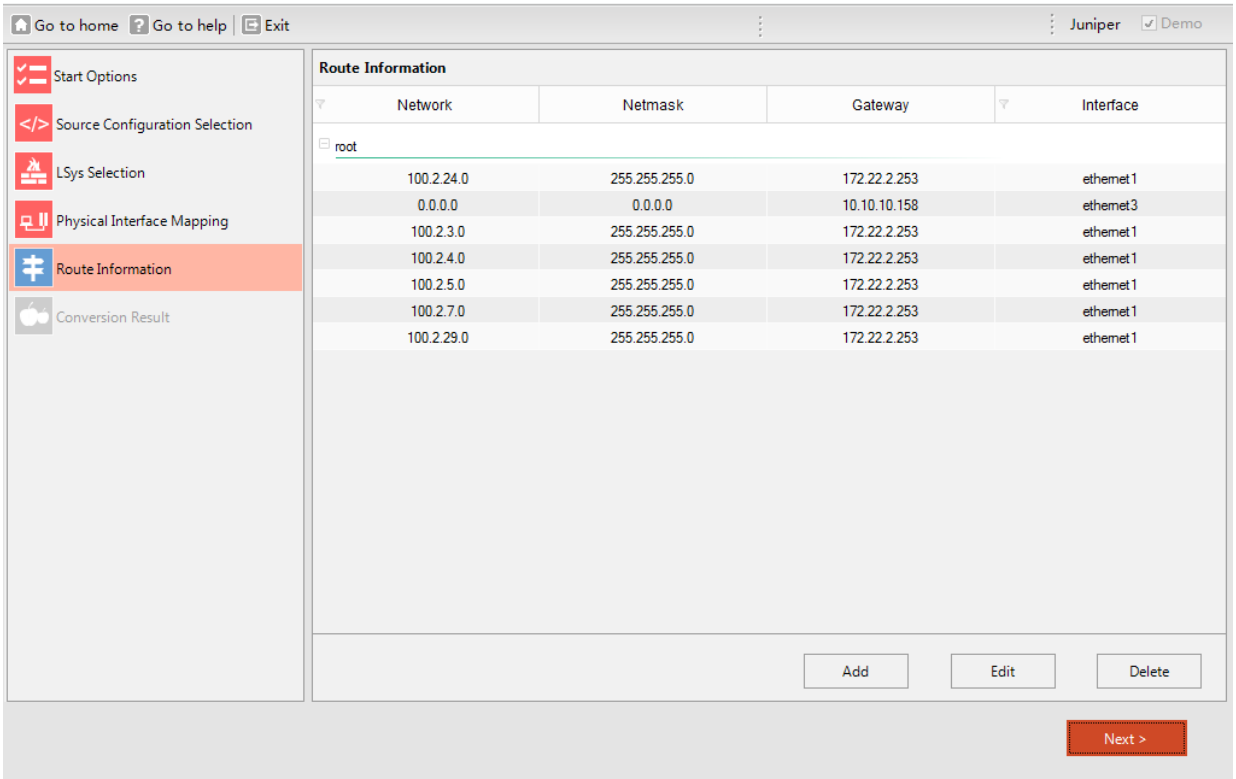
Setting	Description
Select all	Selects or clears all logical virtual system items.
(LSYS or VSYS items)	Select the virtual logical systems to convert.

Physical Interface Mapping



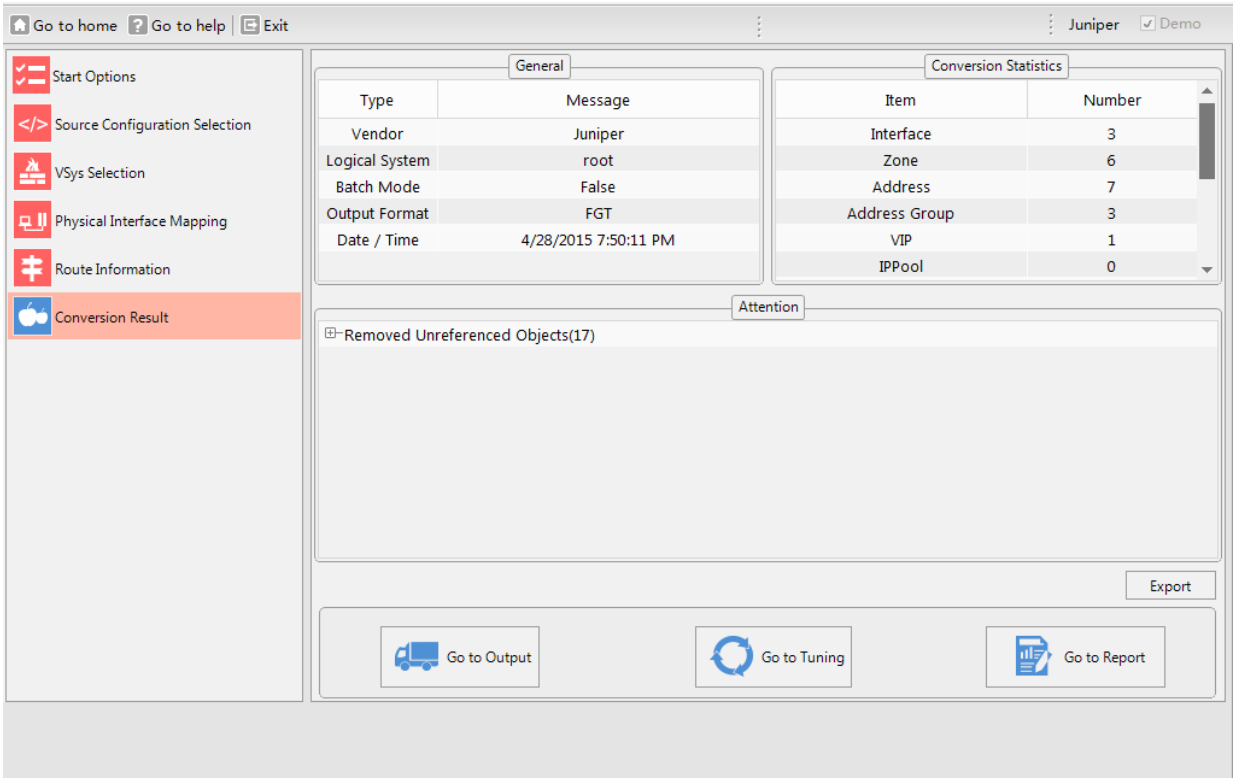
Setting	Description
FG port	Click to assign a FortiGate port for each interface.
(table column)	Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

Route Information



Setting	Description
Add	Click to add a route.
Edit	Click to edit the selected route.
Delete	Click to delete the selected route.

Conversion Result

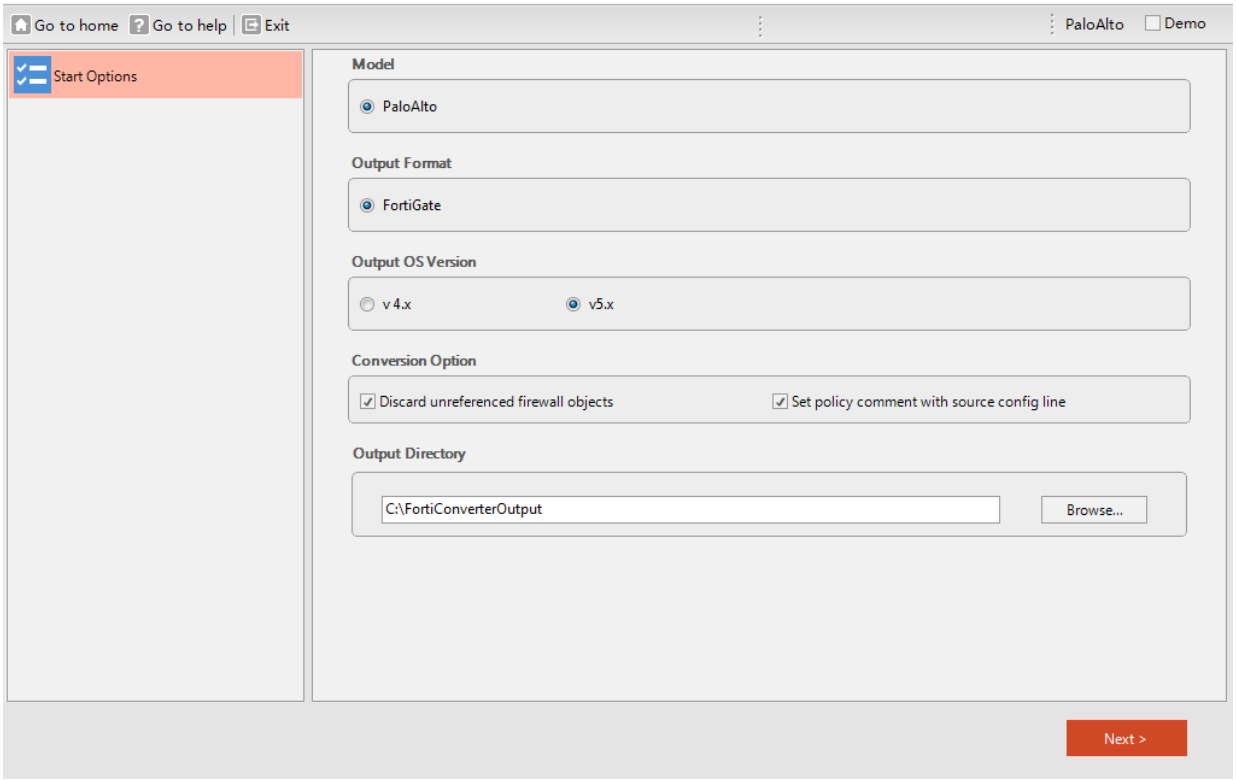


Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81.
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see Viewing the results of your automatic conversion on page 79

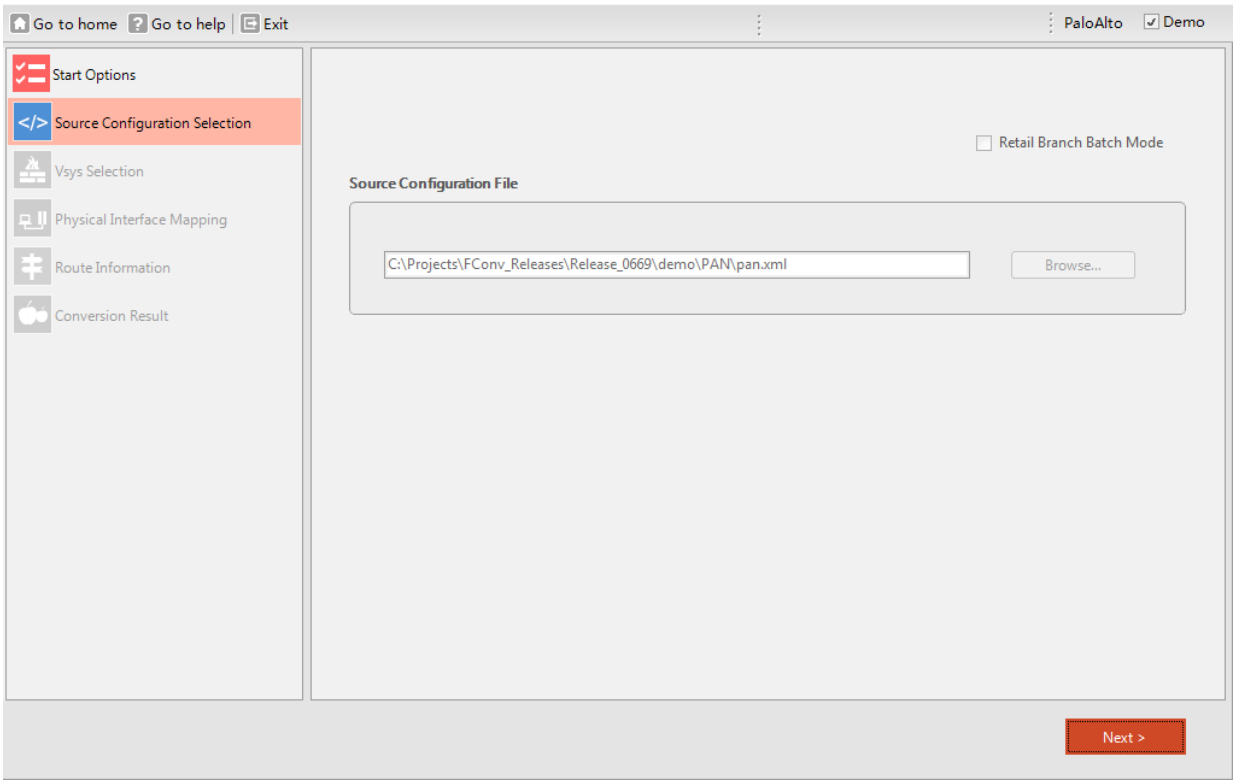
Palo Alto conversion wizard

Start Options



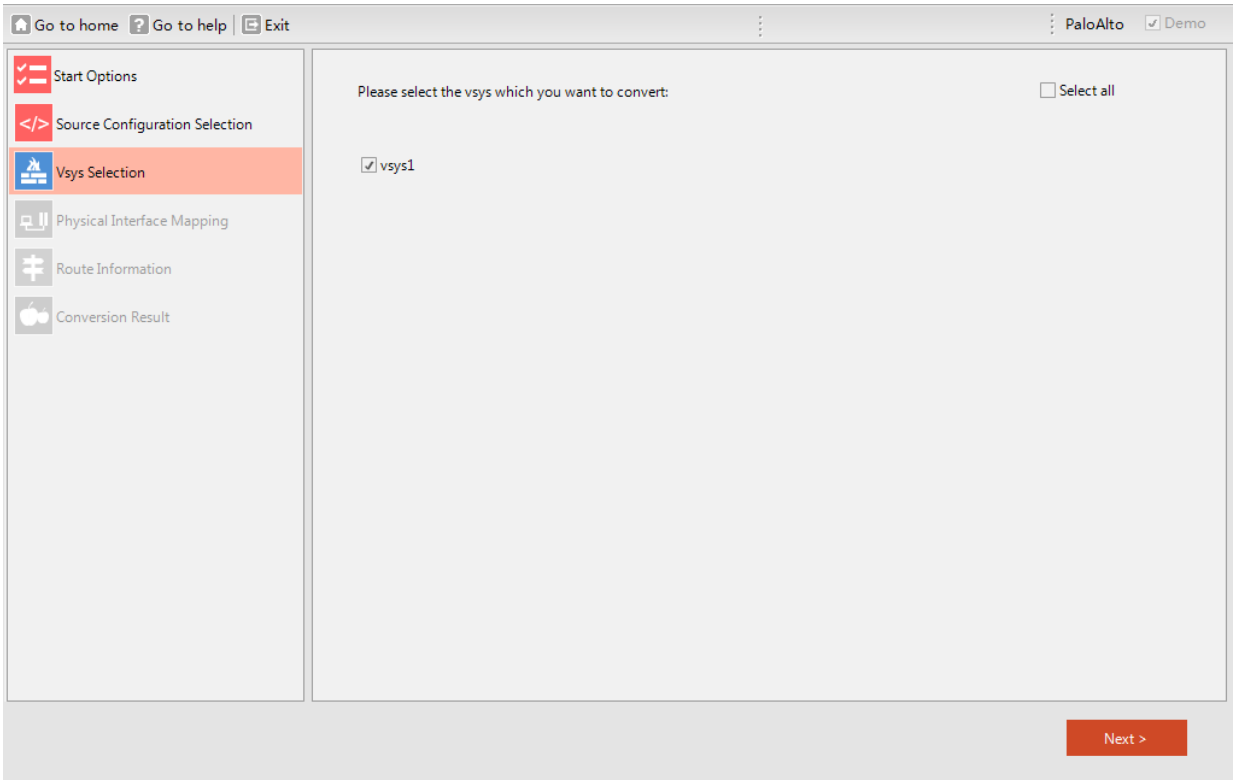
Setting	Description
Model	Palo Alto is the only model supported..
Output Format	FortiGate is the only supported output.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Set policy comment with source config line	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Output Directory	Select the folder where FortiConverter saves the output configuration.

Source Configuration Selection



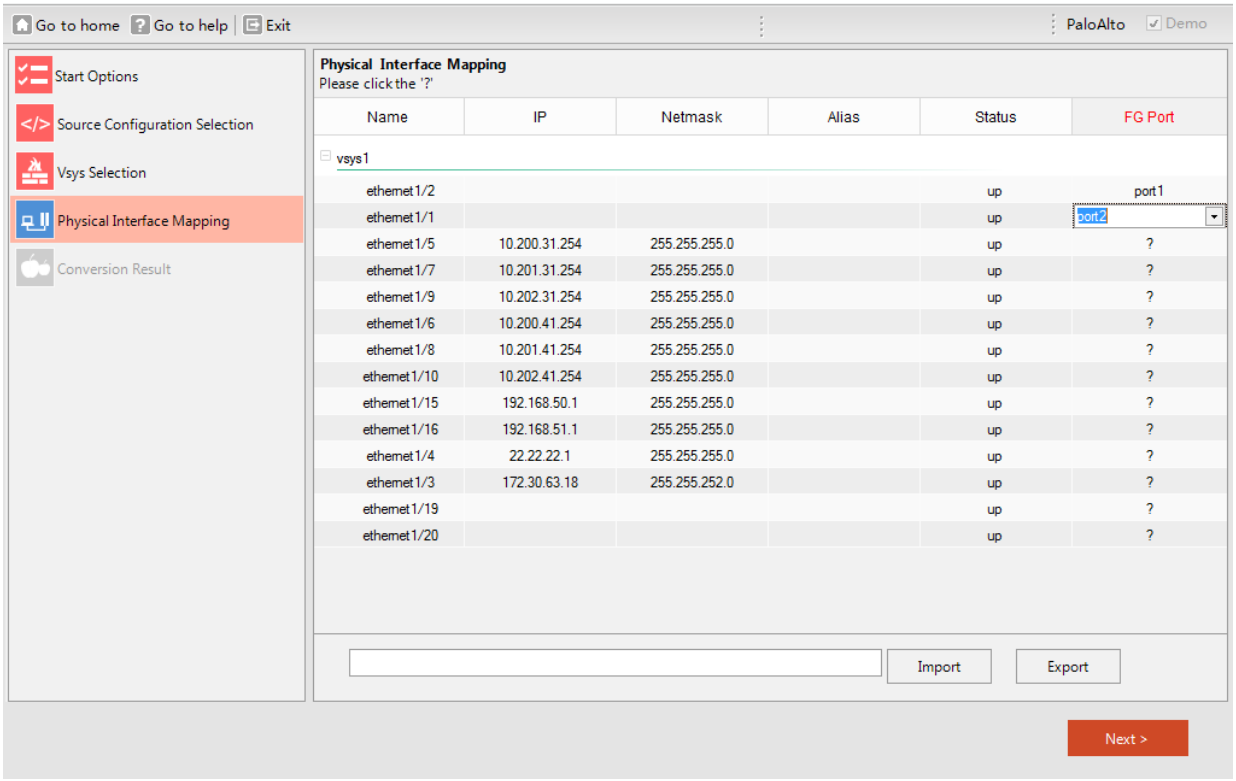
Setting	Description
Retail Branch Batch Mode	Select to specify multiple source configuration files. Ensure that all the source files use the same interface. For more information, see Using retail branch batch conversion mode on page 74
Source Configuration File	Select the input file or files.

VSYS Selection



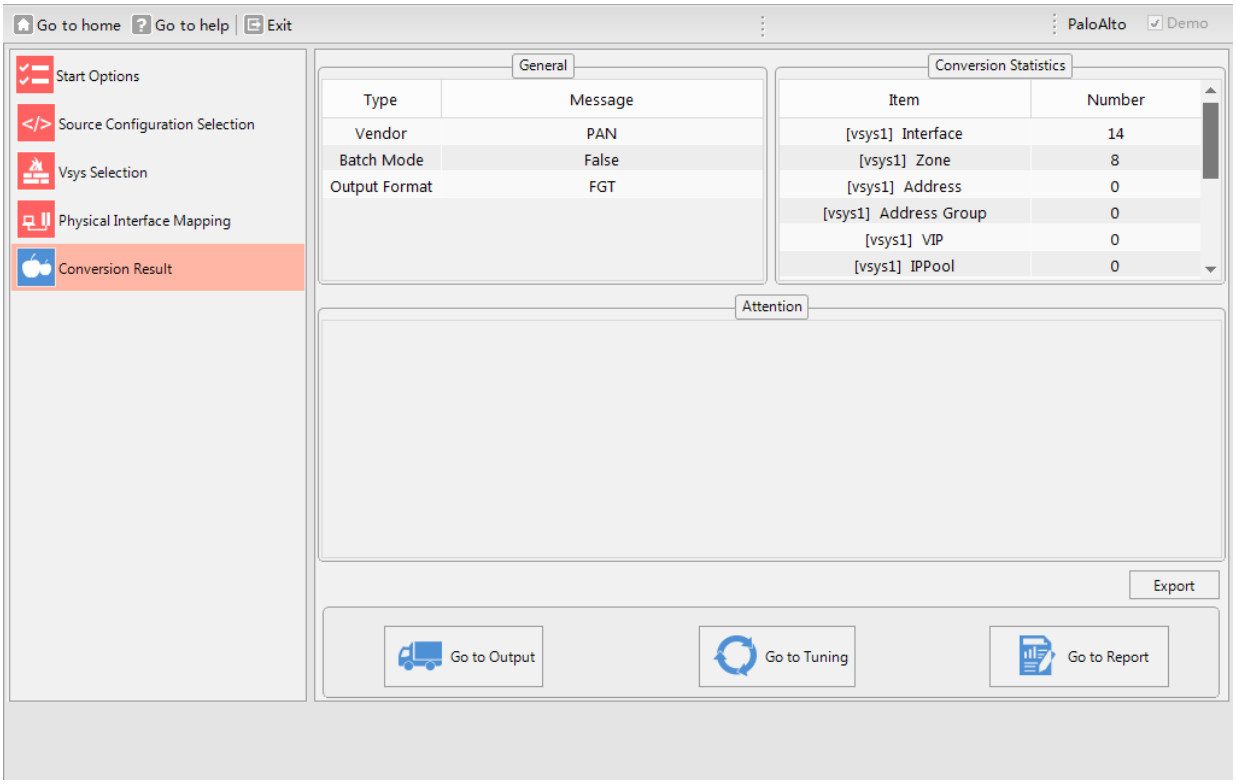
Setting	Description
Select all	Selects or clears all virtual system items.
(VSYS items)	Select the virtual systems to convert.

Physical Interface Mapping



Setting	Description
FG port	Click to assign a FortiGate port for each interface.
(table column)	Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

Conversion Result



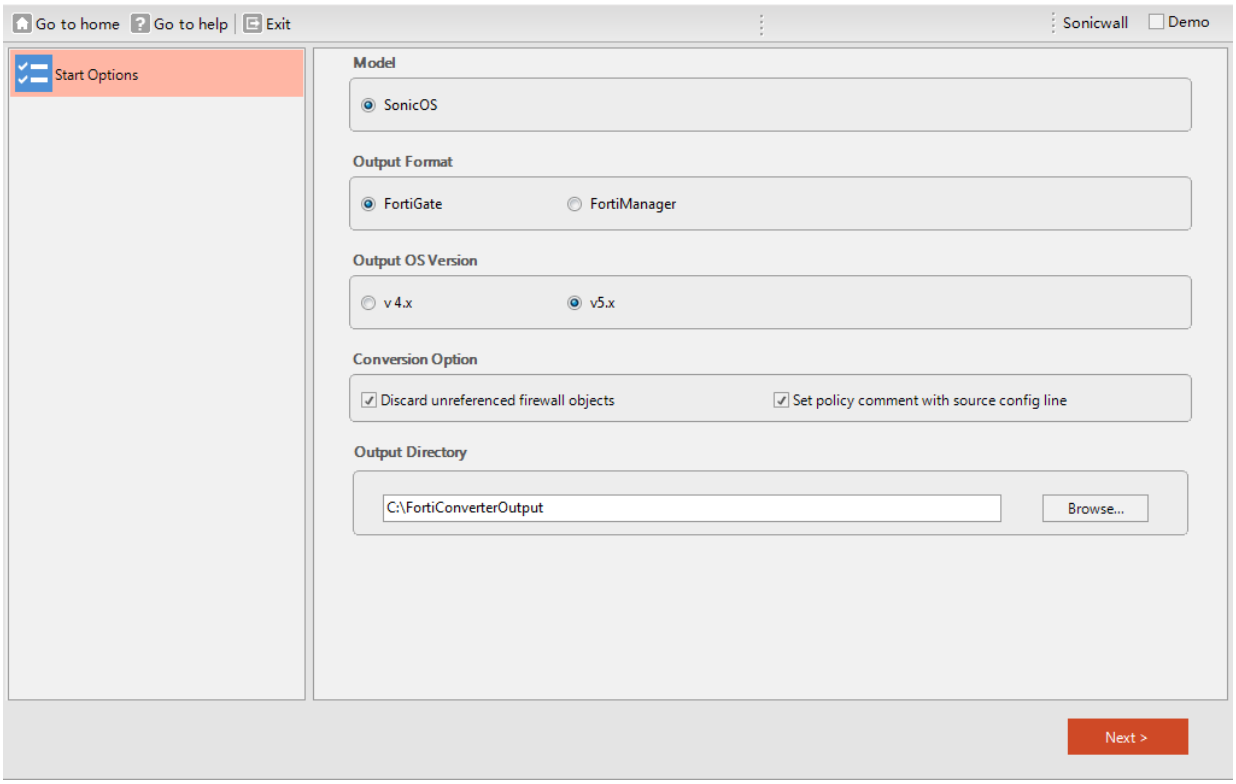
Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81.
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see Viewing the results of your automatic conversion on page 79

SonicWall conversion wizard

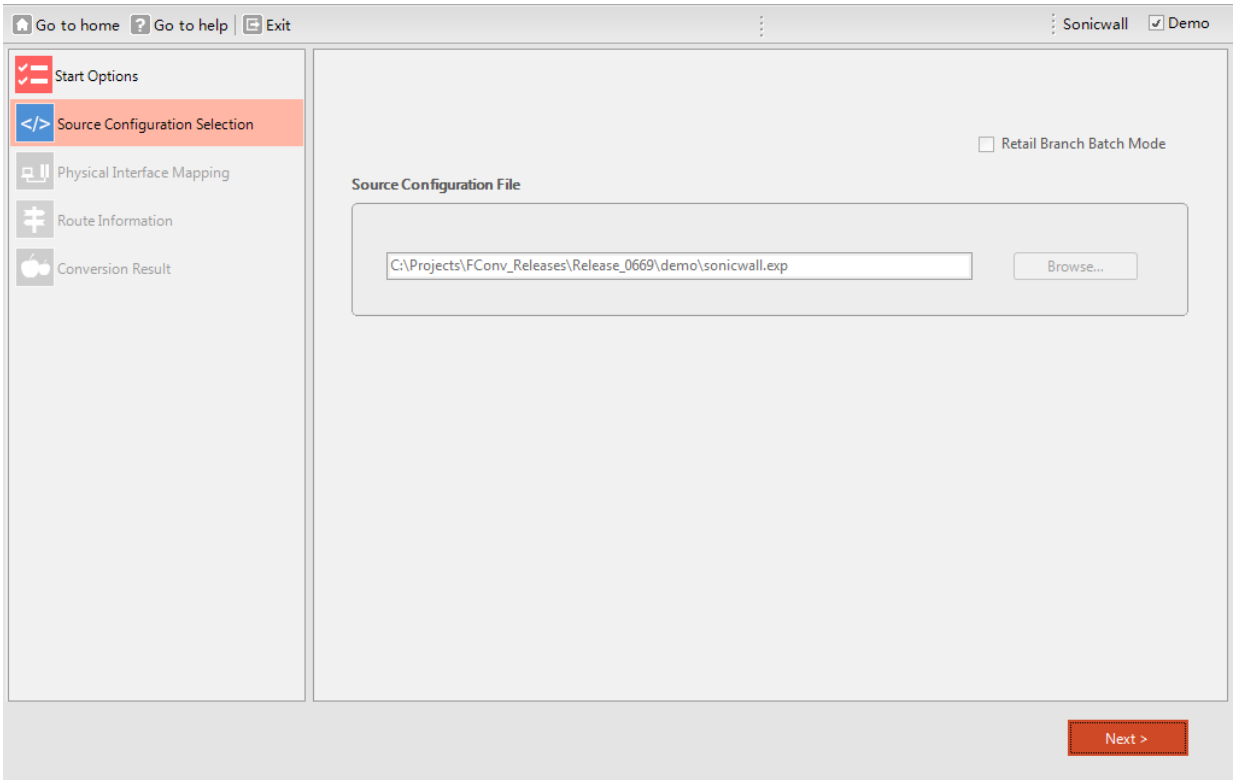
By default, output configurations from SonicWall do not include some configuration information, including address and service comments. For an example of how to include this information in the output, see Including object comments in the output configuration on page 28.

Start Options



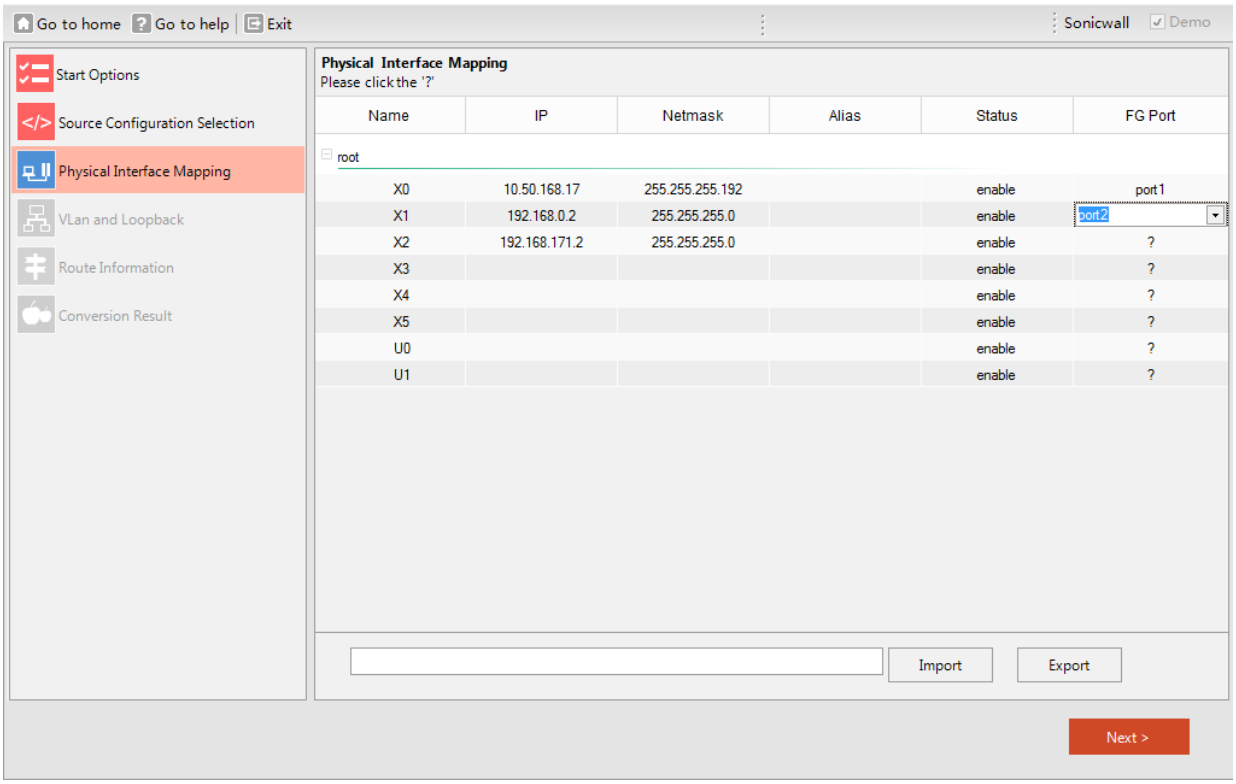
Setting	Description
Model	SonicOS is the only model supported.
Output Format	Select the appropriate output format for your FortiGate device.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Set policy comment with source config line	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Output Directory	Select the folder where FortiConverter saves the output configuration.

Source Configuration Selection



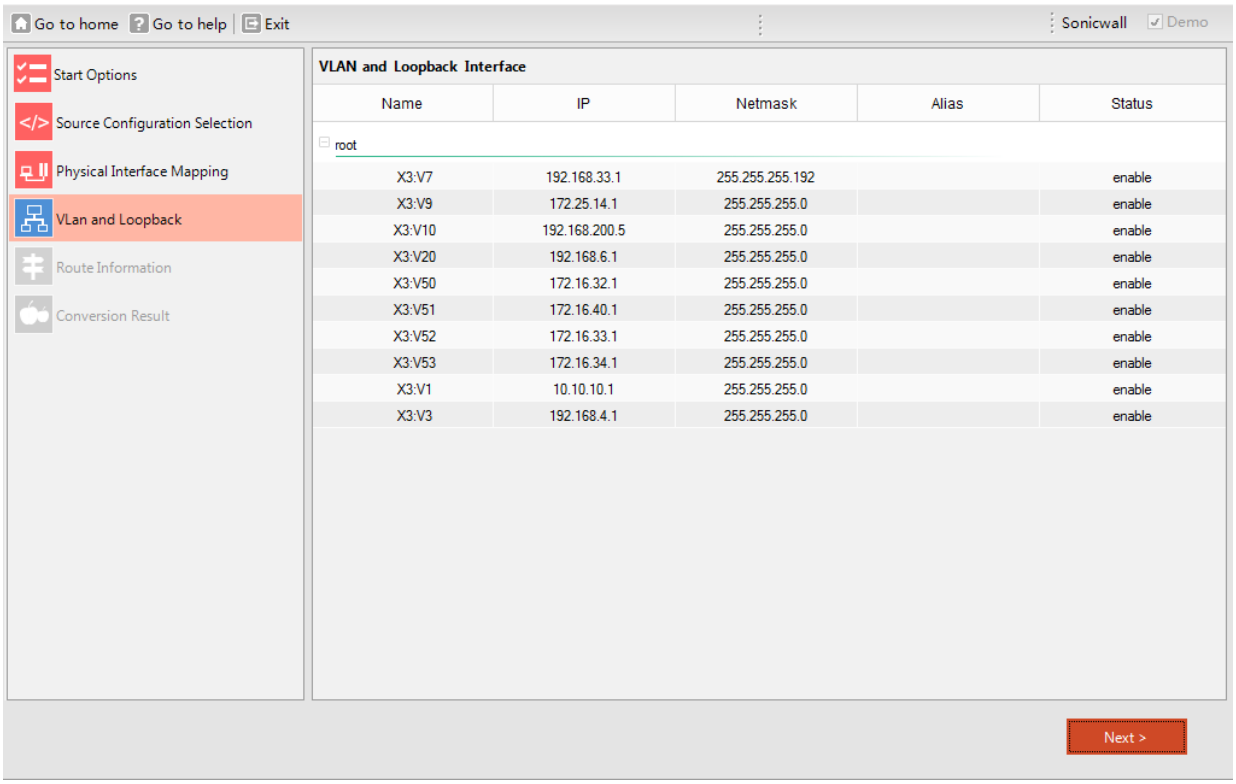
Setting	Description
Retail Branch Batch Mode	Select to specify multiple source configuration files. Ensure that all the source files use the same interface. For more information, see Using retail branch batch conversion mode on page 74
Source Configuration File	Select the input file or files.

Physical Interface Mapping



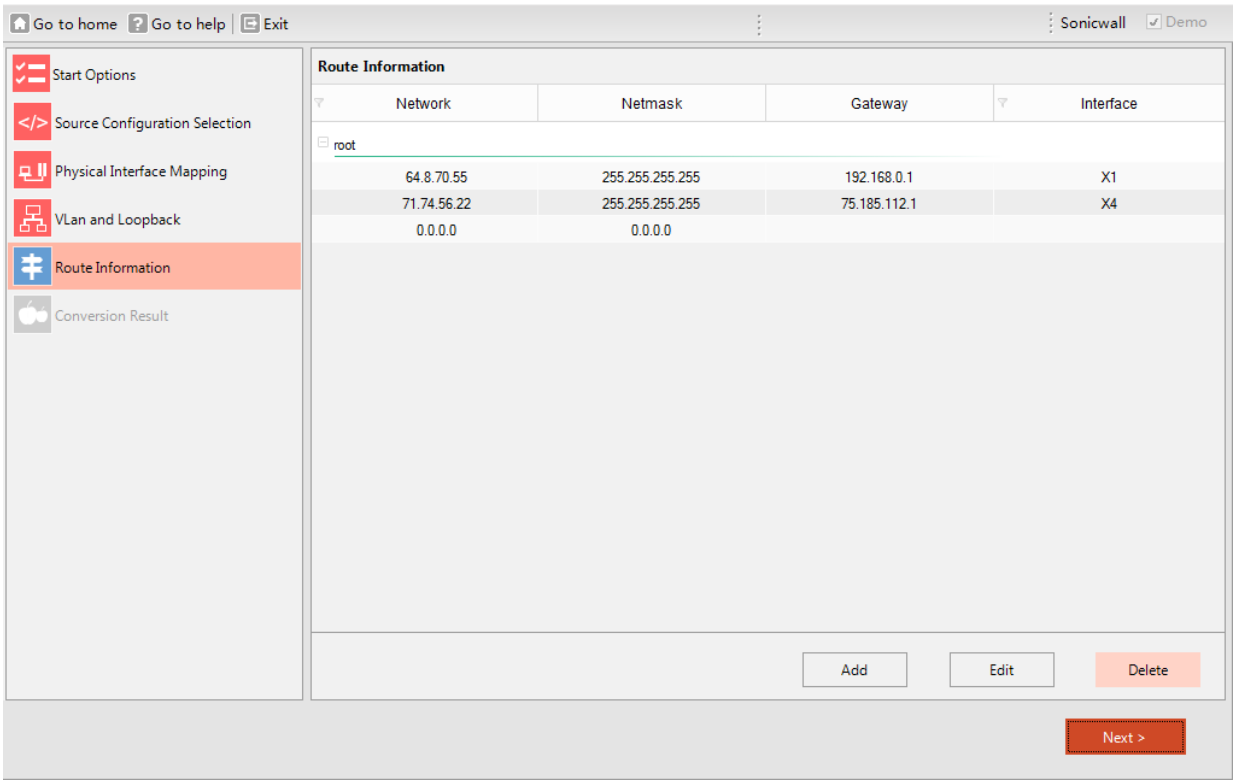
Setting	Description
FG port	Click to assign a FortiGate port for each interface.
(table column)	Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

VLAN and Loopback



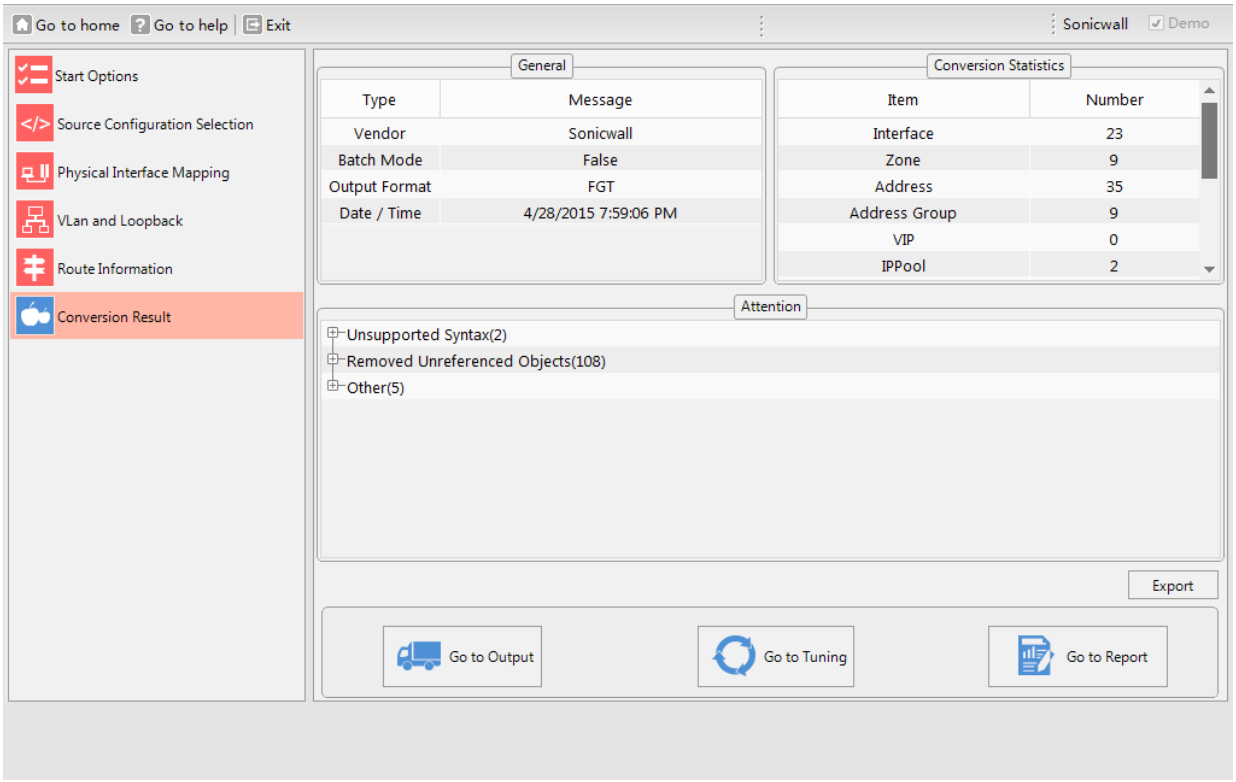
For information only. No settings.

Route Information



Setting	Description
Add	Click to add a route.
Edit	Click to edit the selected route.
Delete	Click to delete the selected route.

Conversion Result

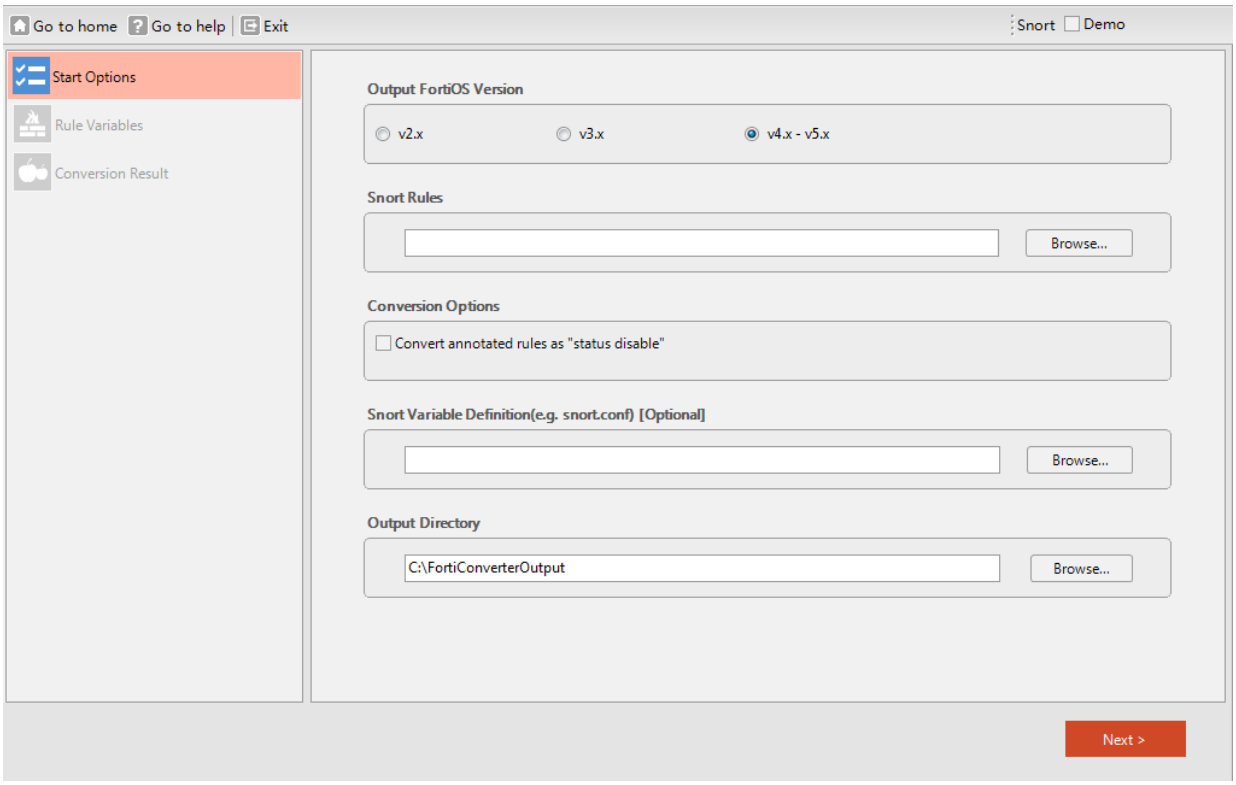


Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81.
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see Viewing the results of your automatic conversion on page 79

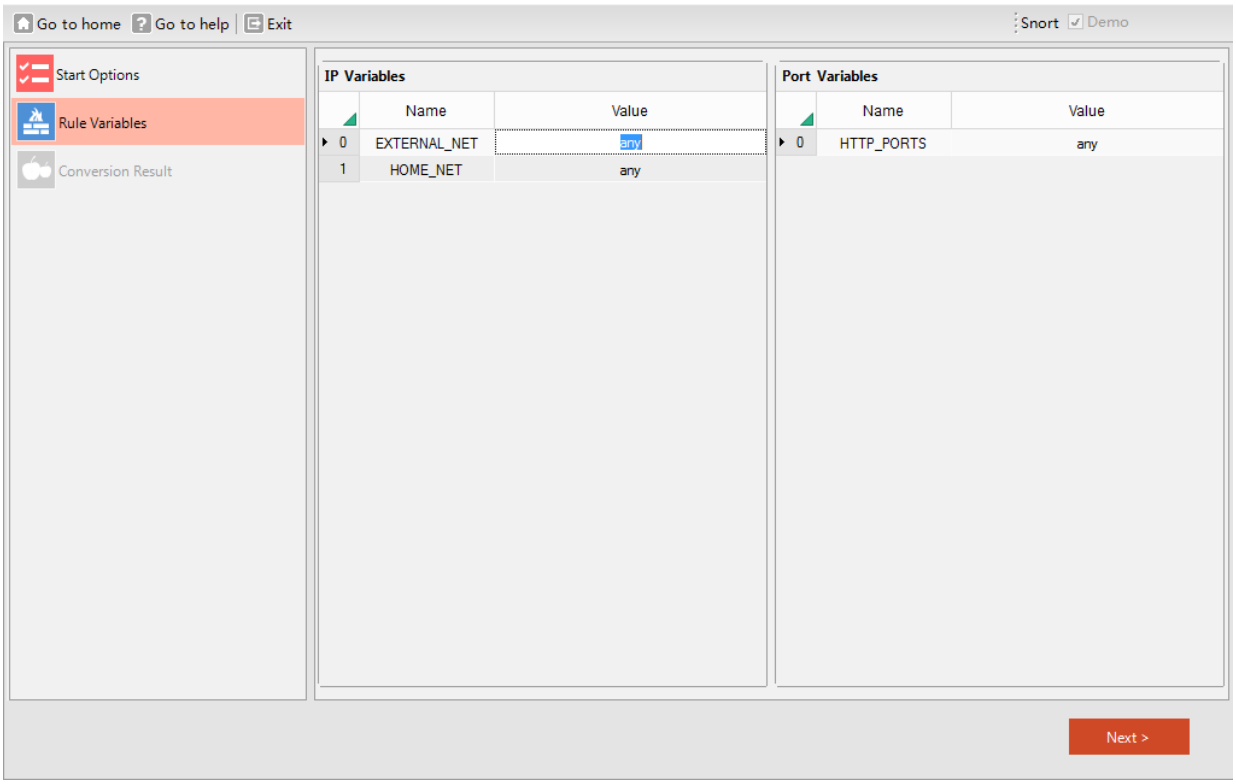
Snort conversion wizard

Start Options



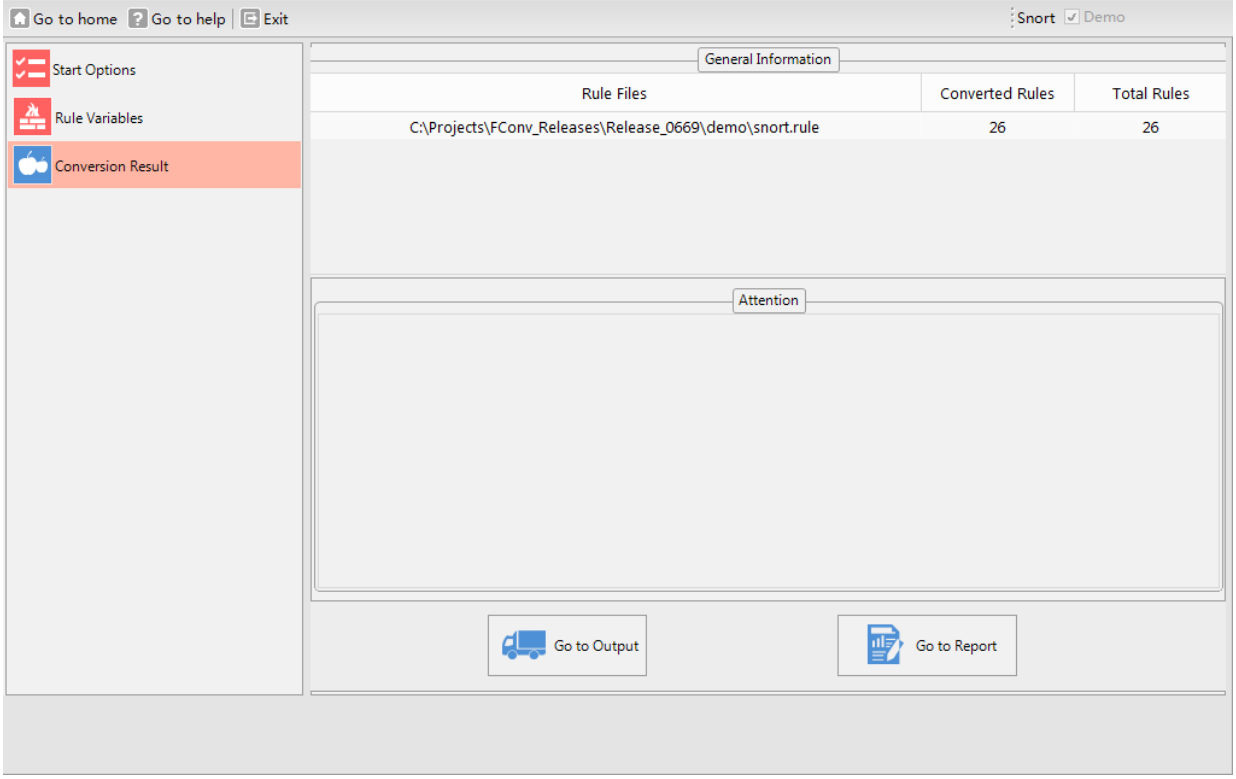
Setting	Description
Output FortiOS Version	FortiOS 2.x, 4.x, and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Snort Rules	Select the input file.
Convert annotated rules as "status disable"	Select to disable rules that are annotated in the source configuration.
Snort Variable Definition	Optionally, select the Snort variable definition file (for example, `snort.conf`)
Output Directory	Select the folder where FortiConverter saves the output configuration.

Rule Variables



Setting	Description
IP Variables	Click a value to edit it, if required.
Port Variables	Click a value to edit it, if required.

Conversion Result



Setting	Description
Go to Output	Opens the output folder .
Go to Report	Opens an HTML page that displays the conversion mapping.

For more information, see Viewing the results of your automatic conversion on page 79

Using retail branch batch conversion mode

In the retail industry and other sectors, enterprises often deploy the same firewall configuration at a large number of remote sites. Instead of converting each site individually, the FortiConverter **Retail Branch Batch Mode** option allows you to use the wizard to convert all these sites in a single operation.

Typically, these firewall configurations have one or two network interfaces that connect to a WAN and differ only in the specified LAN and WAN IP addresses, the device name, and a few configuration objects.

Because the batch mode converts the specified group of configurations to a FortiGate configuration with a standard interface mapping, it requires that all the source configurations have the same number of network interfaces. The wizard applies the **FG Port** values that you specify in the wizard's physical port mapping settings to all the output configurations. If any of the source configurations you select have a different number of interfaces, the wizard displays an alert.

Most of the conversion wizard steps are the same as when you convert a single configuration. However, the fine tuning feature you can use to edit the conversion configuration is not available in batch mode.

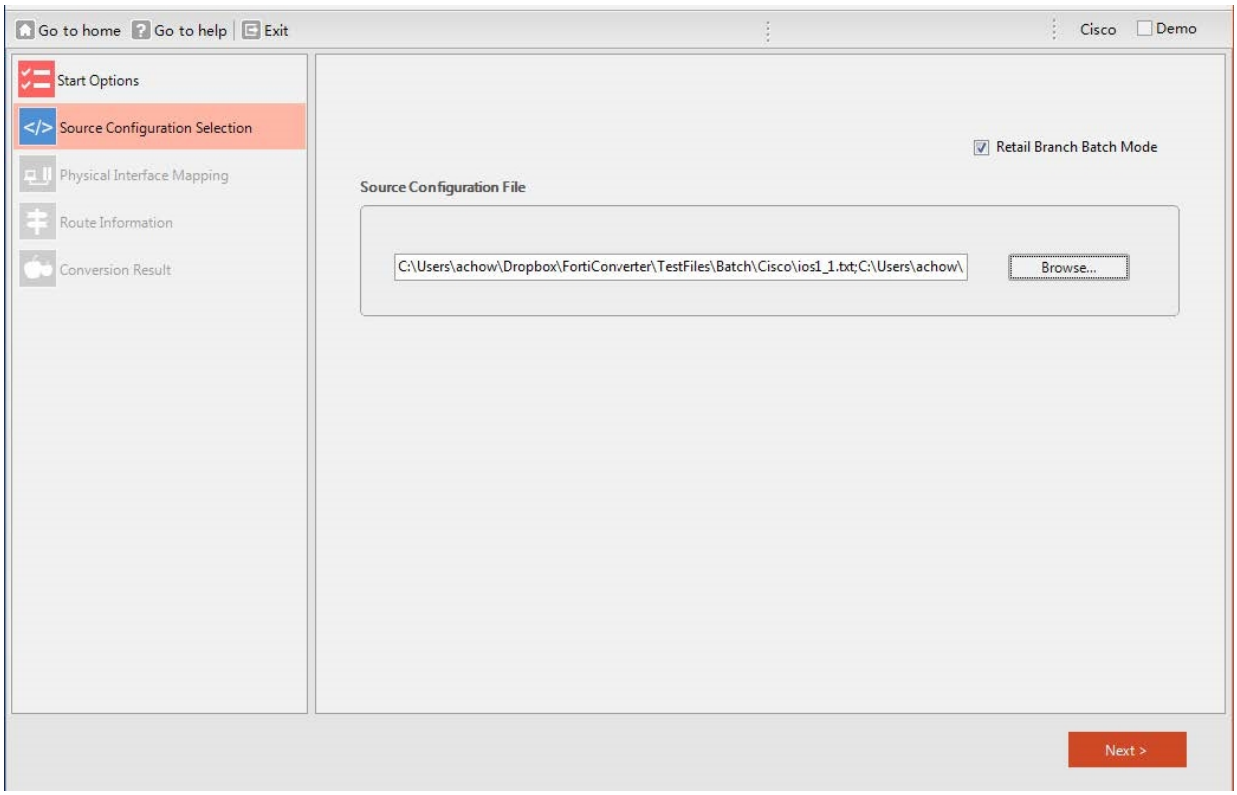
If any of your sites has a unique configuration or needs to be customized (for example, a firewall at the head office), do not use the **Retail Branch Batch Mode** option. Instead, see the instructions for converting a single configuration for your source firewall.

Batch mode for Cisco, Juniper, Palo Alto Networks, and SonicWall firewalls

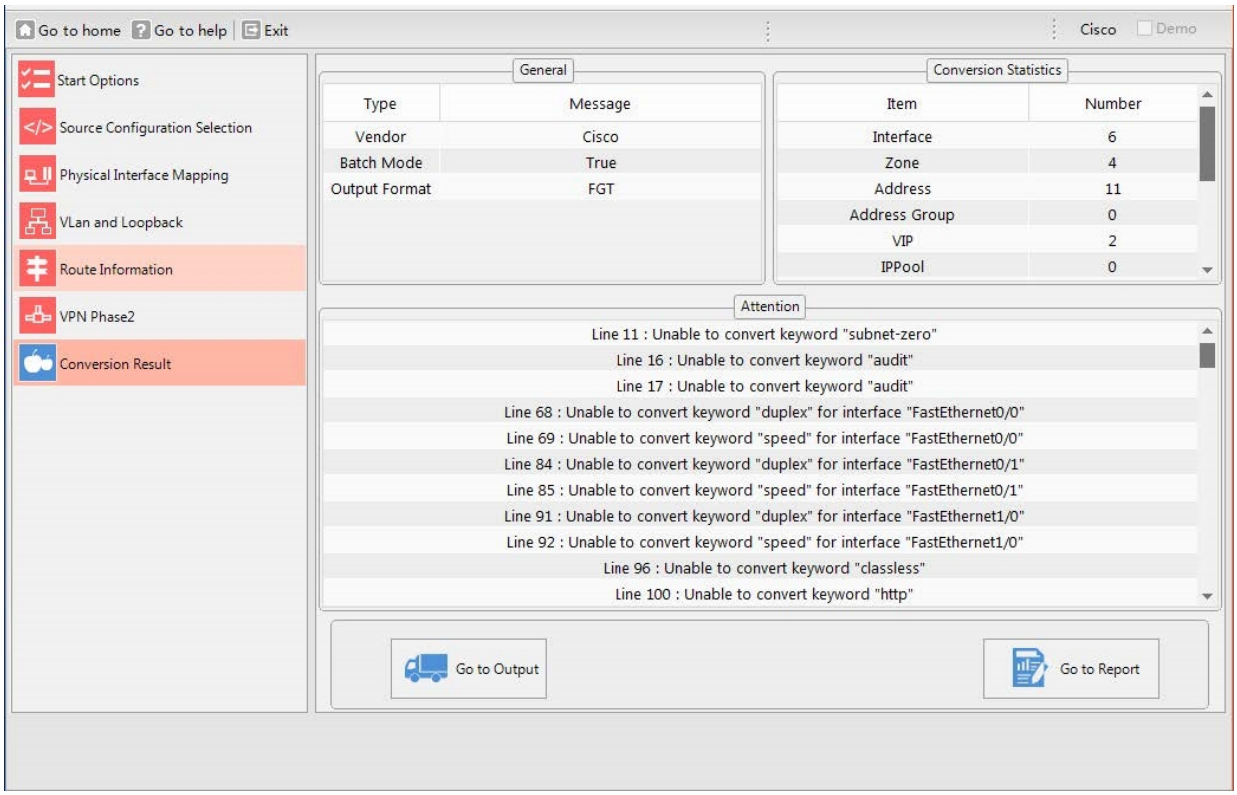
To enable batch mode when you convert Cisco, Juniper, Palo Alto Networks, and SonicWall firewalls, on the wizard's Source Configuration Selection page, select **Retail Branch Batch Mode**.

Click **Browse** to navigate to and select the configuration files. You can select multiple files.

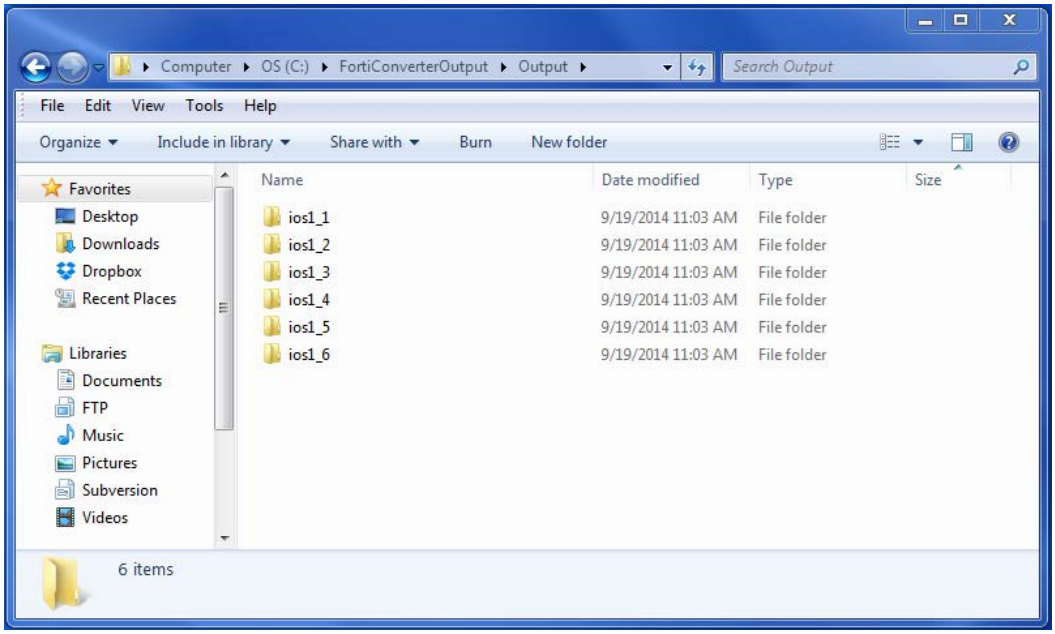
The wizard displays the selected files in a single line in the **Source Configuration File** field.



All other steps for using the wizard at the same as when you convert a single configuration, except for the **Conversion Result** page, which does not display the **Go to Tuning** option.



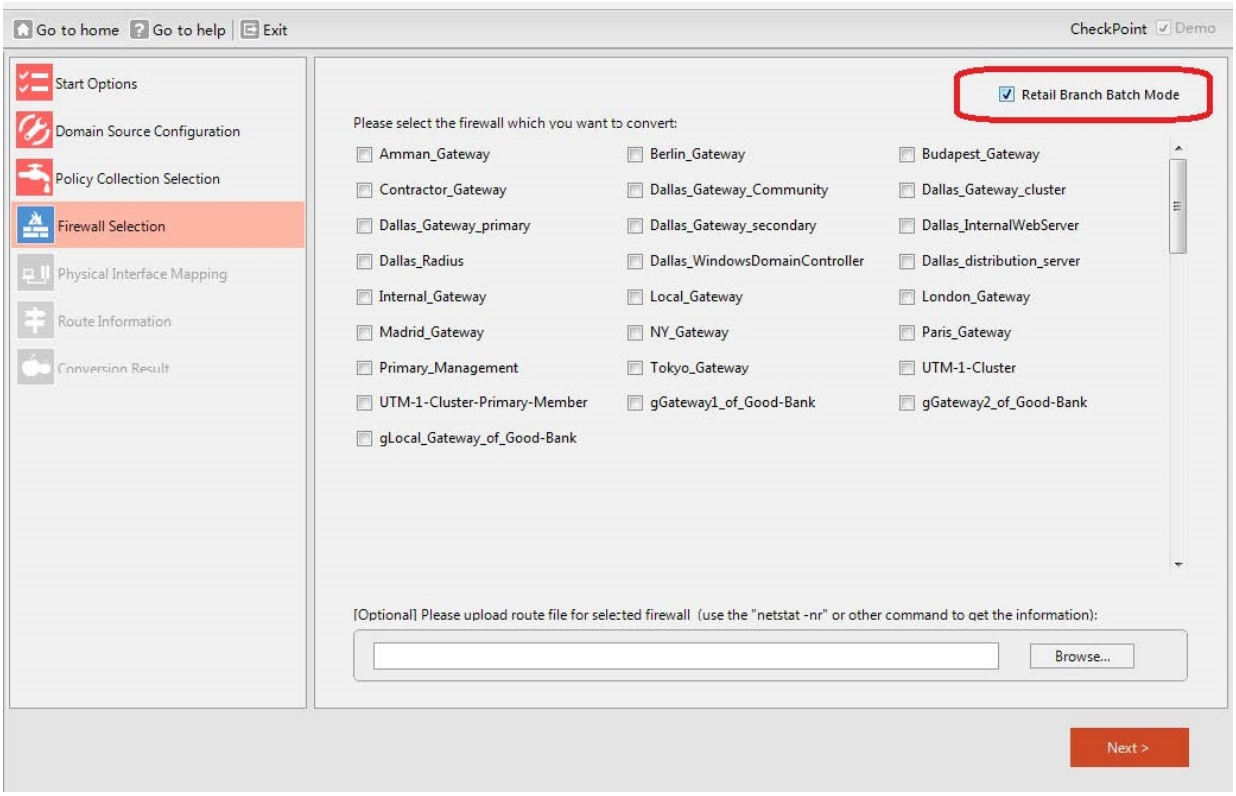
For batch conversion, the wizard saves each configuration file in its own directory in the output directory.



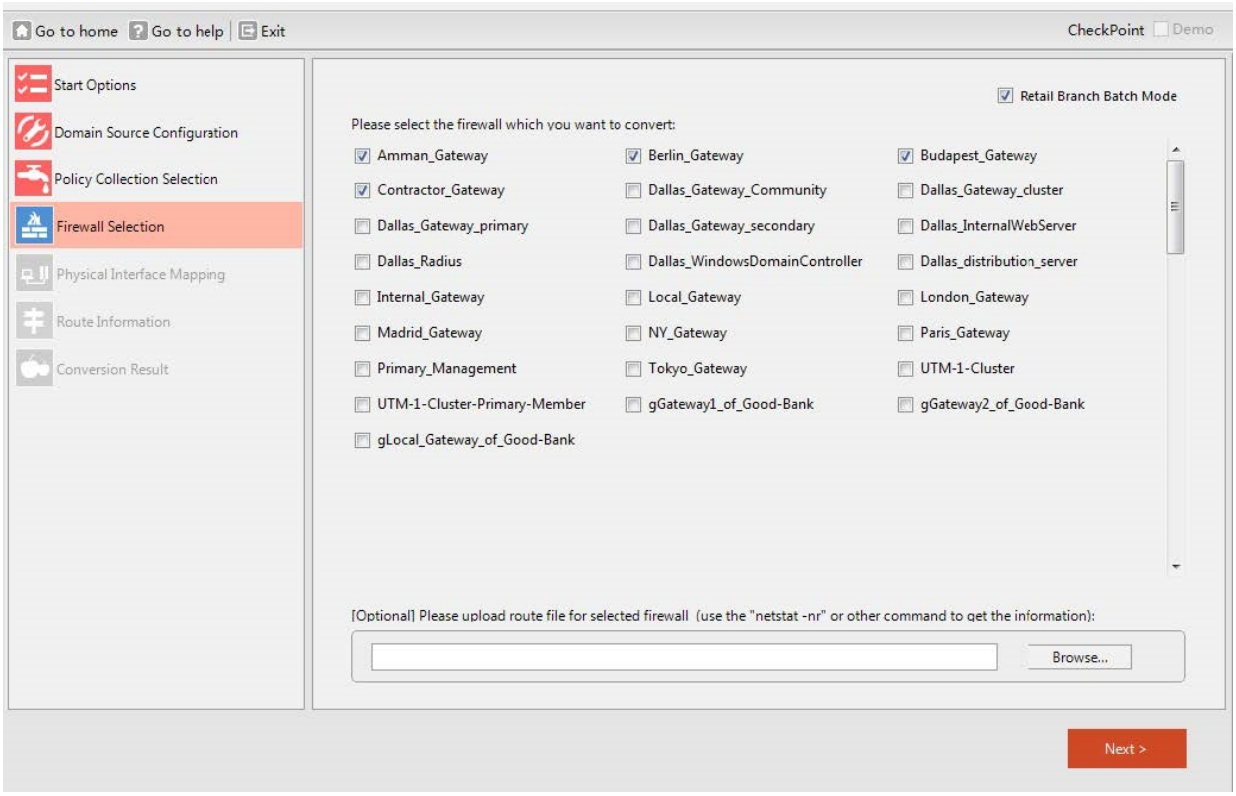
Batch mode for Alcatel-Lucent and Check Point firewalls

For Check Point and Alcatel-Lucent firewalls, batch mode can convert multiple firewalls within a configuration. You select the same input configuration and output settings as when you convert a single configuration. Then, on

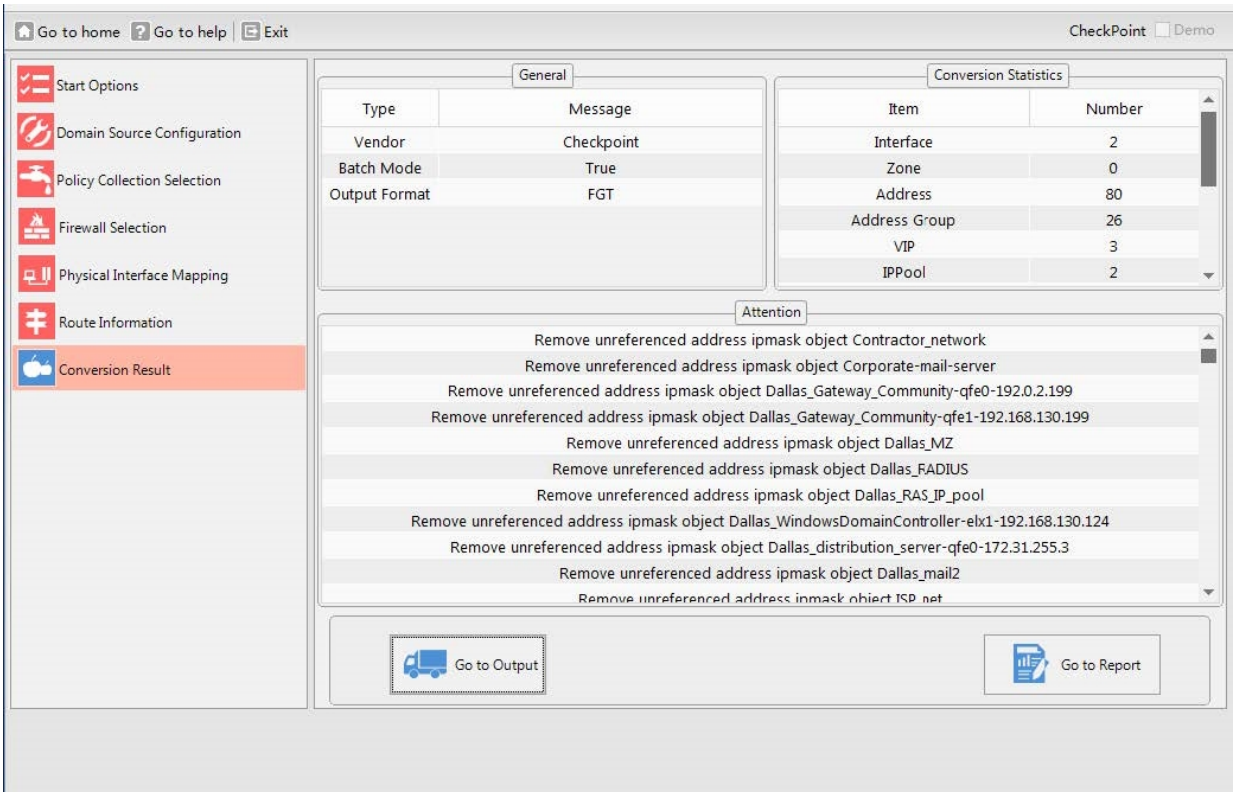
the Firewall Selection page (Check Point) or Device Selection page (Alcatel-Lucent), select **Retail Branch Batch Mode**.



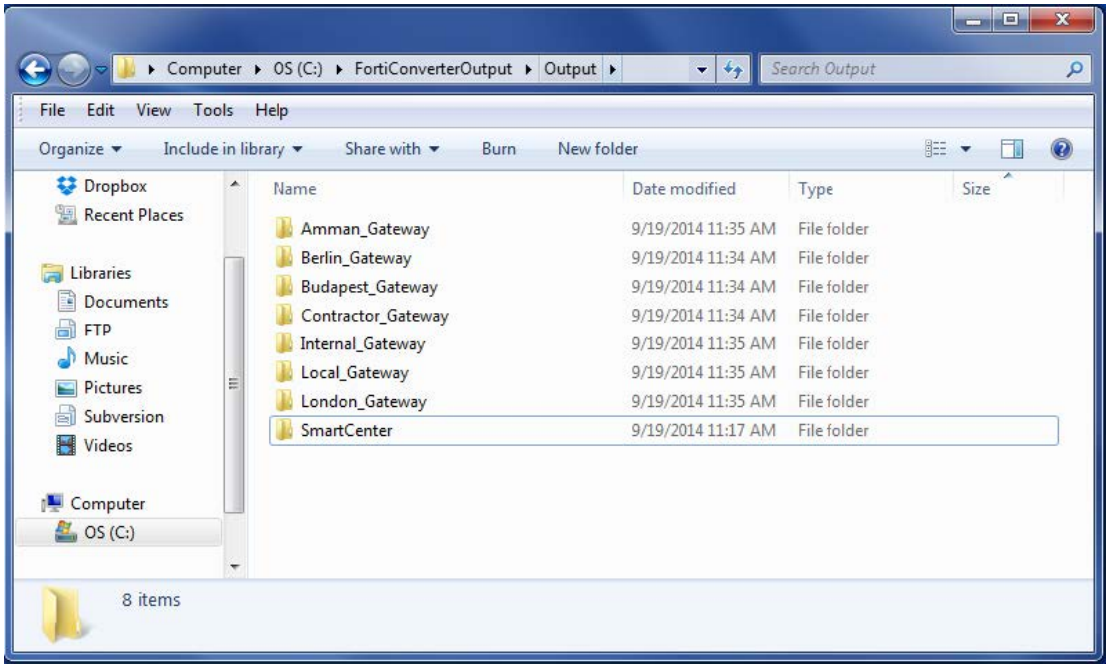
Select the firewalls to convert. Batch conversion requires that all the firewalls have the same number of network interfaces.



All other steps for using the wizard at the same as when you convert a single configuration, except for the **Conversion Result** page, which does not display the **Go to Tuning** option.



For batch conversions, the wizard saves each configuration file in its own directory in the output directory.

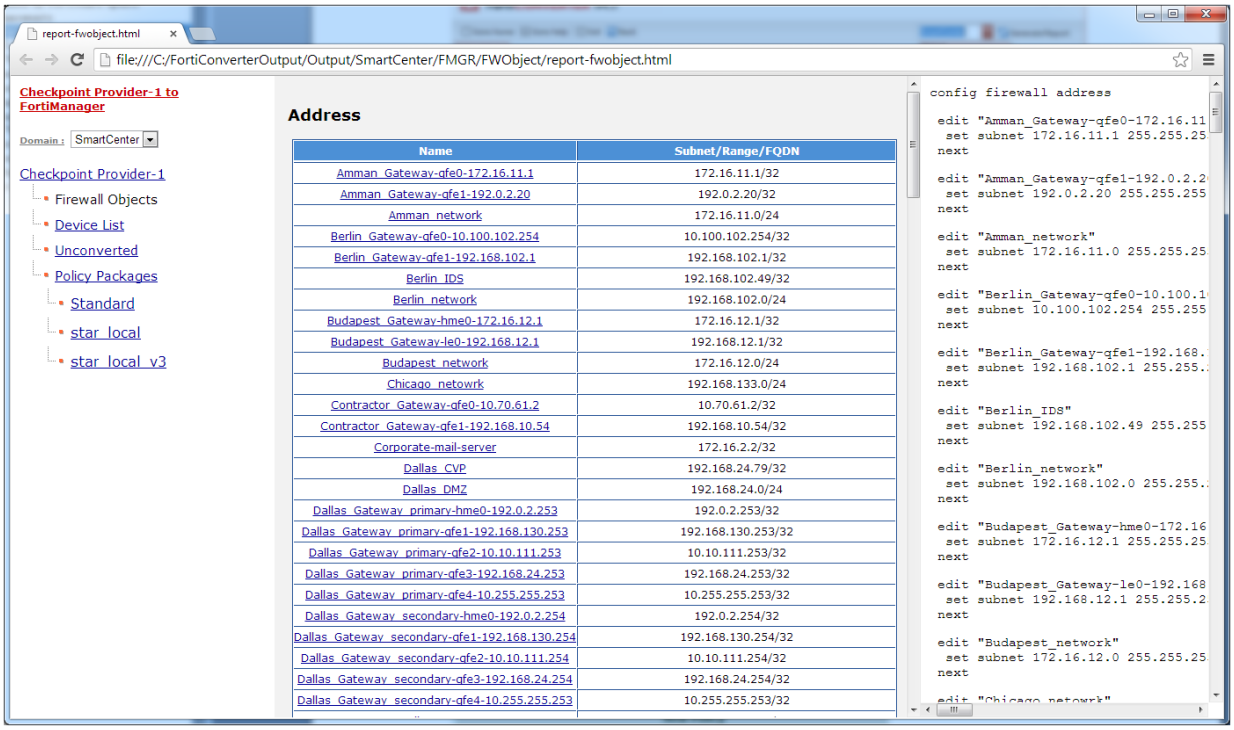


Viewing the results of your automatic conversion

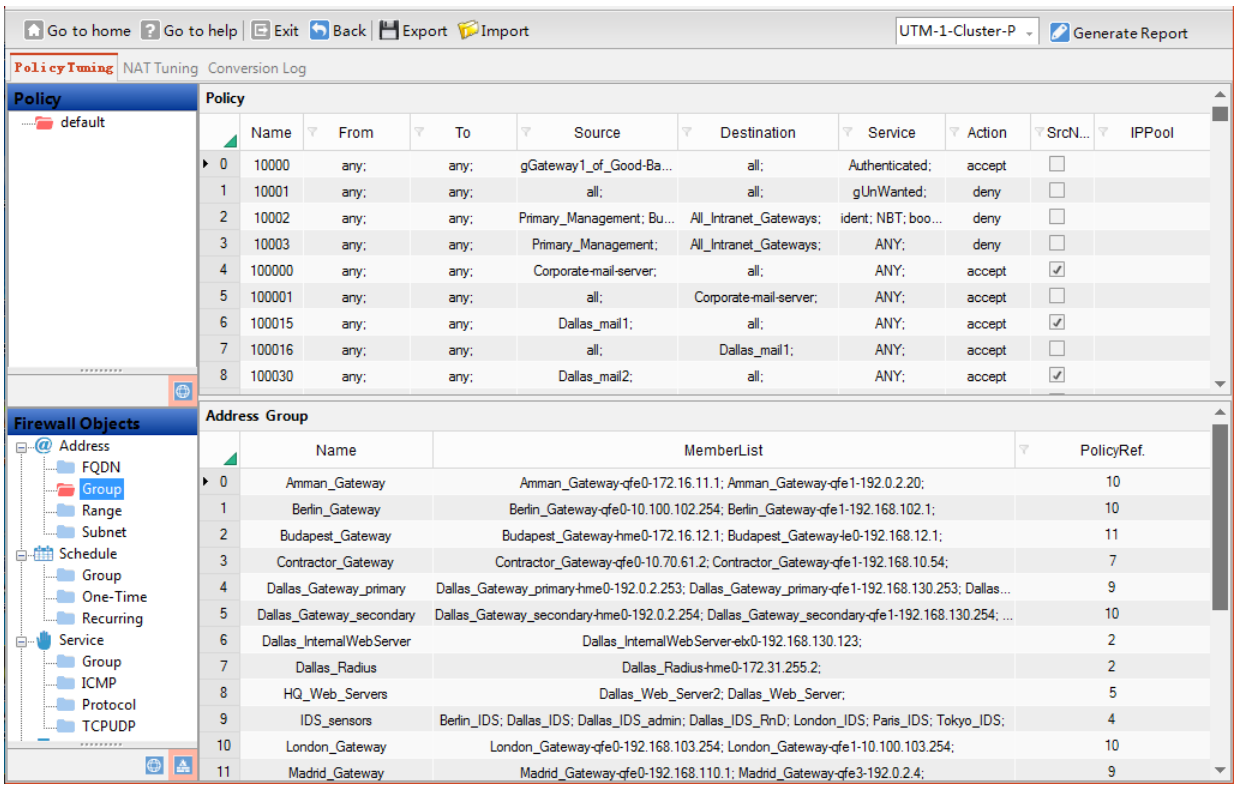
The Conversion Result page displays general conversion information, statistics on of the number of converted objects and policies, and a log of items that need further attention.

To see a summary of the conversion, click **Go to Report**.

An HTML page generated by FortiConverter is displayed in your web browser.



To examine the converted objects and policies in detail, click **Go to Tuning**. A window that allows you to tune the output is displayed.

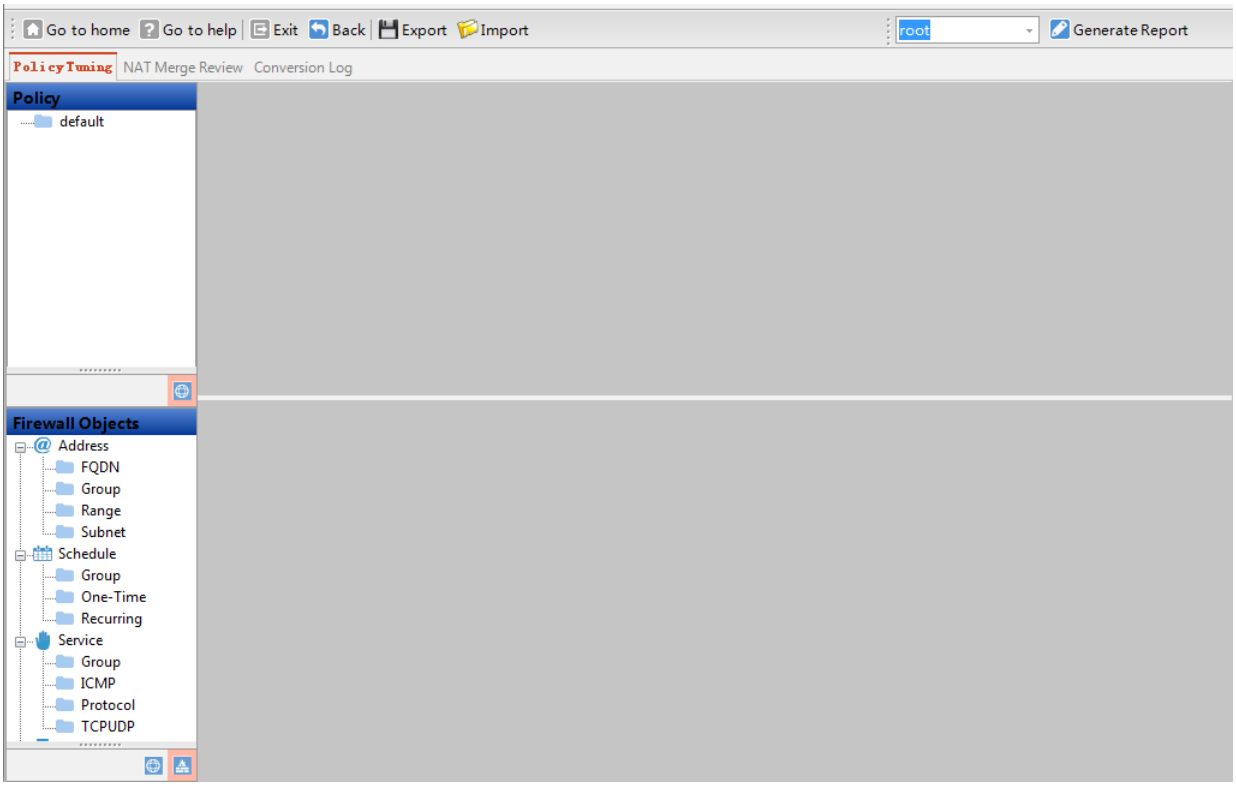


After your review and any tuning tasks are complete, click **Go to Output** to access the final, converted configuration files.

Tuning the FortiConverter output

Although FortiConverter attempts to automatically convert as much of the source configuration as possible, in some cases, your input is required to complete the conversion. The Tuning page allows you to tune the results for your environment. To access the Tuning page, on the Conversion Result page, click **Go to Tuning**.

To quickly view a tuning "snapshot" (a configuration that you exported from the tuning page earlier), open the wizard for the appropriate vendor, click **Tuning** on any page, and then navigate to the snapshot file to import it.



Toolbar options

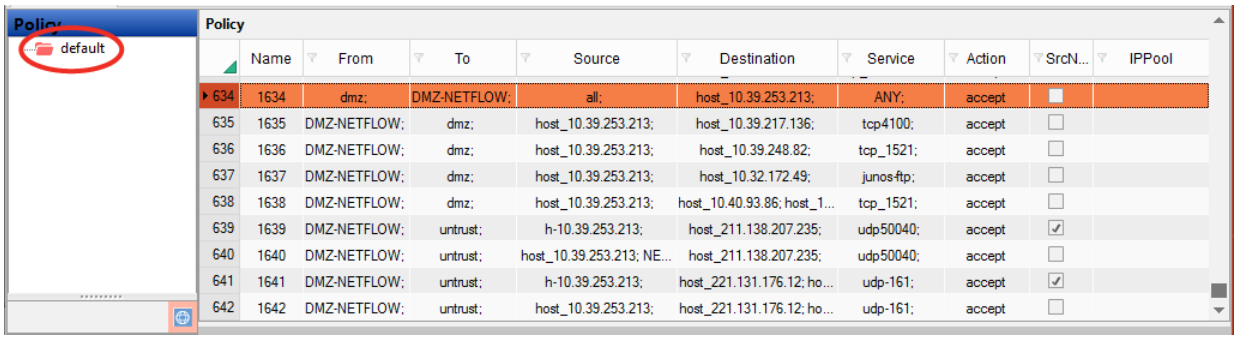
Item	Description
Go to home	Click to return to the main page.

Item	Description
Go to help	Click to open the latest version of this guide.
Exit	Click to close FortiConverter.
Back	Click to return to the Conversion Result page. FortiConverter preserves any changes but does not save them in an output file. (Use **Generate Report** to save changes to an output file.)
Export	Click to save the current configuration, including any modifications, to a text file (a tuning "snapshot").
Import	Click to import a configuration you exported earlier (a tuning "snapshot"). FortiConverter discards any changes in the current configuration.
VDOM	Select the VDOM in the output to display in the Tuning page.
Generate Report	Click to export the current configuration, including any modifications to an output configuration file .

Policy Tuning tab

The Policy Tuning tab allows you to review output policies and converted objects.

To review output policies, in the Policy navigation pane, select a package. The converted policies in the package are displayed.

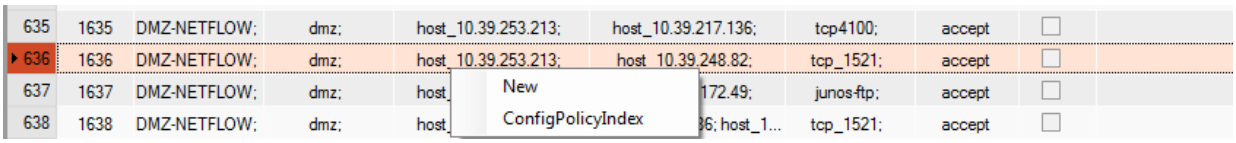


To add a new policy to a package

1. Right-click a policy, and then click **New**.
2. Complete the settings, and then click **OK**.

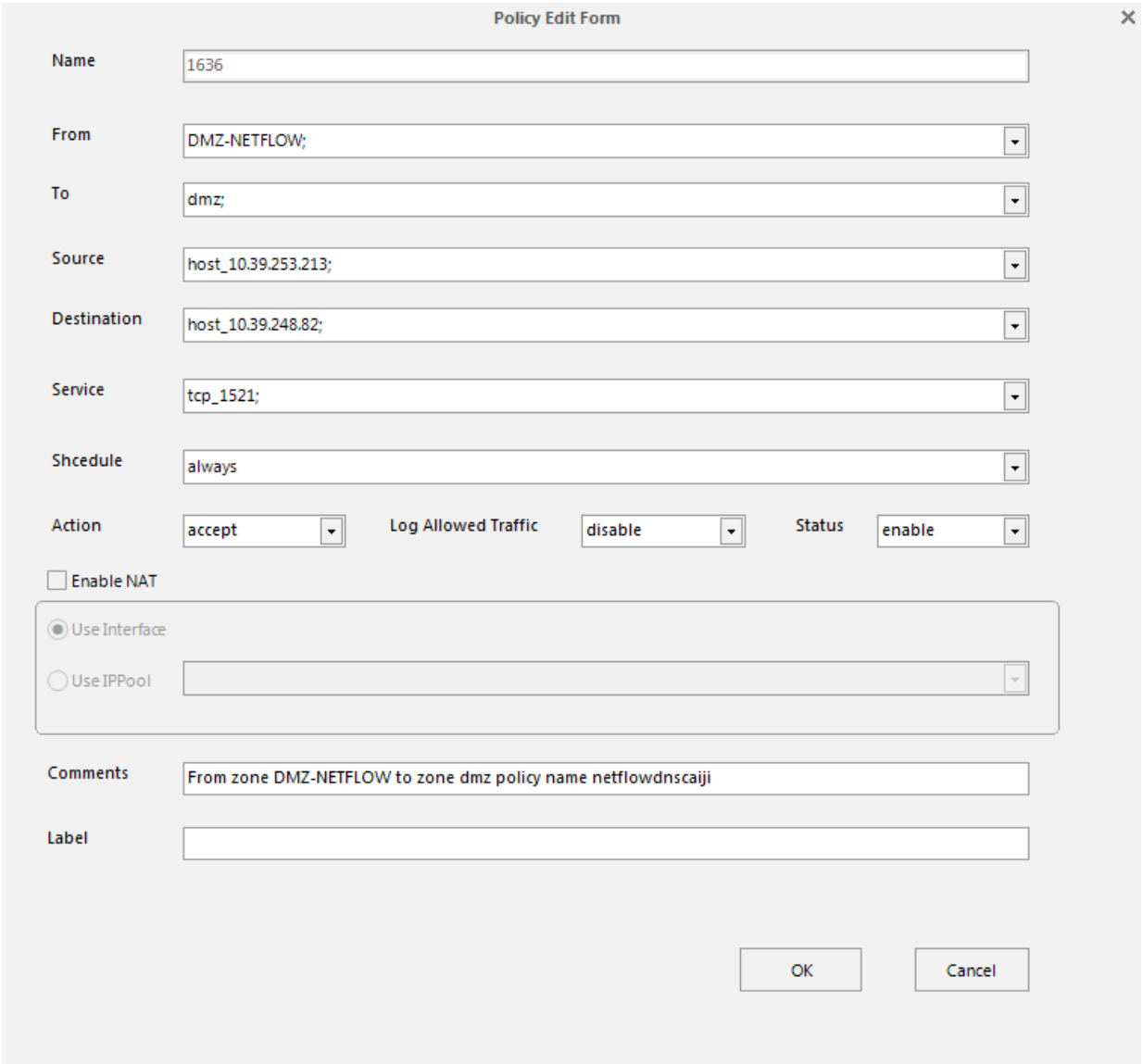
To renumber the policies

1. Right-click the policy where you want the numbering to restart, and then click **ConfigPolicyIndex**.
2. For **Set Policy Index Start With**, enter the initial policy number to use, and then click **OK**.



To edit the details for a converted policy

Double-click the policy and edit the settings as required.



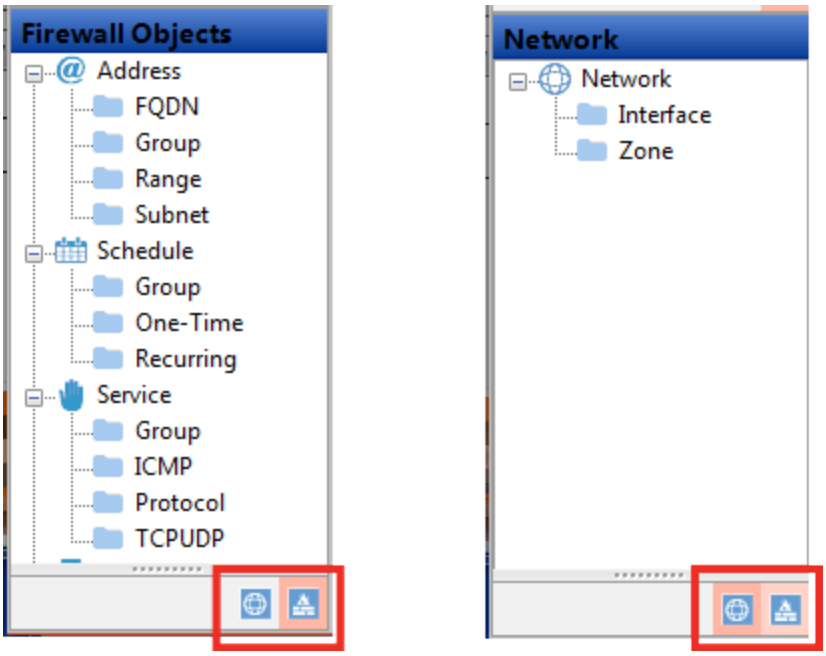
Item	Description
Name	You cannot edit this value.
From	Select source interface(s).

Item	Description
To	Select destination interface(s).
Source	Select source address object(s).
Destination	Select destination address object(s).
Service	Select service object(s).
Schedule	Select schedule object. – select to enable NAT, and then select to use Interface or IPPool Comments – modify the comments for the policy Label – modify the label of the policy
Action	Specify whether traffic is accepted or denied.
Log Allowed Traffic	Specify whether logging is enabled.
Status	Specify whether the policy is enabled.
Enable NAT	Select to enable NAT, and then do one of the following: • Select **User Interface**. • Select **Use IPPool** and specify a pool.
Comments	Edit the comments for the policy.
Label	Edit the label for the policy.

To review and edit firewall objects and interfaces

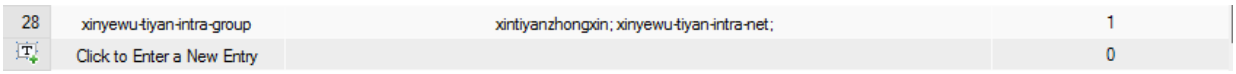
1. Go to the navigation pane at the bottom-left of the Policy Tuning tab.

   Click the icons at the bottom of the pane to switch between firewall objects and interfaces.



2. To view objects, select a category in the navigation pane.

3. To add a new object, scroll to the bottom of the list, click in an empty row, and then complete the fields as required.



4. The PolicyRef column displays the number of policies that reference that firewall object.

   Click the PolicyRef. column for the entry to display the specific policies in the Policy table above.

   You cannot delete objects that are referenced by any other part of the configuration.

To filter rows to display only matching data

You can filter every column that has the [filter mark] by a given option or custom expression.

To delete a line of the configuration

Click the policy or object you want to delete to select it, and then press the Delete key.

You cannot delete items that are used by another policy or group.

To reorder rows

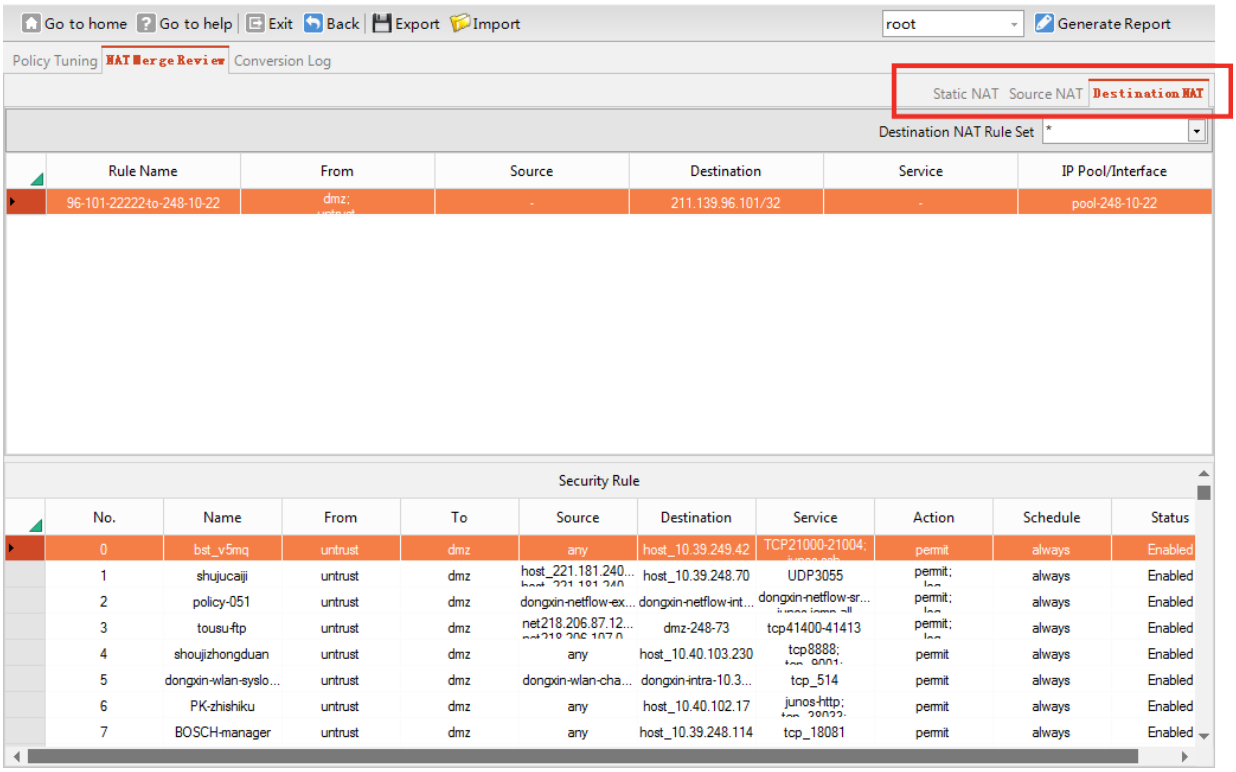
To reorder rows, click the policy number and drag the row to the new position.

NAT Merge Review tab

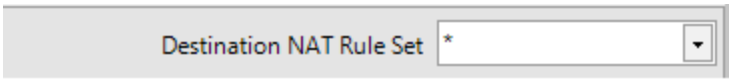
Currently, the NAT Merge Review tab allows you to review of the NAT policy conversion logic for Check Point and Juniper Junos OS conversions only.

Junos NAT Merge Review

You can use the sub-tabs in the top-right corner to select the NAT category to display: Source NAT, Destination NAT, Static NAT, Object NAT, Double NAT, and NAT Rule. The source configuration determines which categories are available.

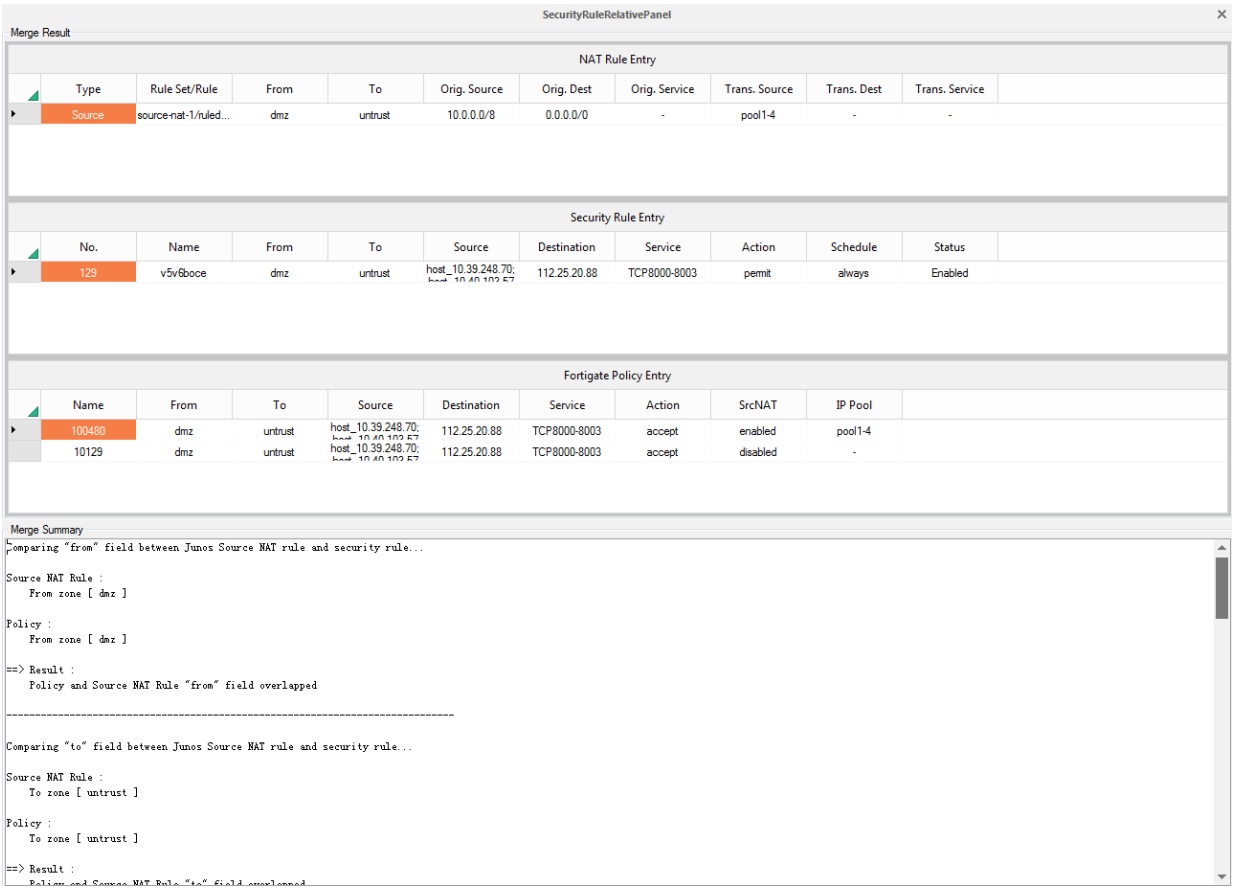


To display a particular rule set from the source configuration, for **Destination NAT Rule Set**, select the appropriate value.



The top pane of the NAT Merge Review tab is a list of NAT rules from the source configuration. Double-click a NAT rule to display the corresponding items in the Security Rule list (bottom pane).

Double-click a security rule to open the Merge Result window.



The Merge Result window displays the NAT rule, the security rule, and the resulting FortiGate policies.

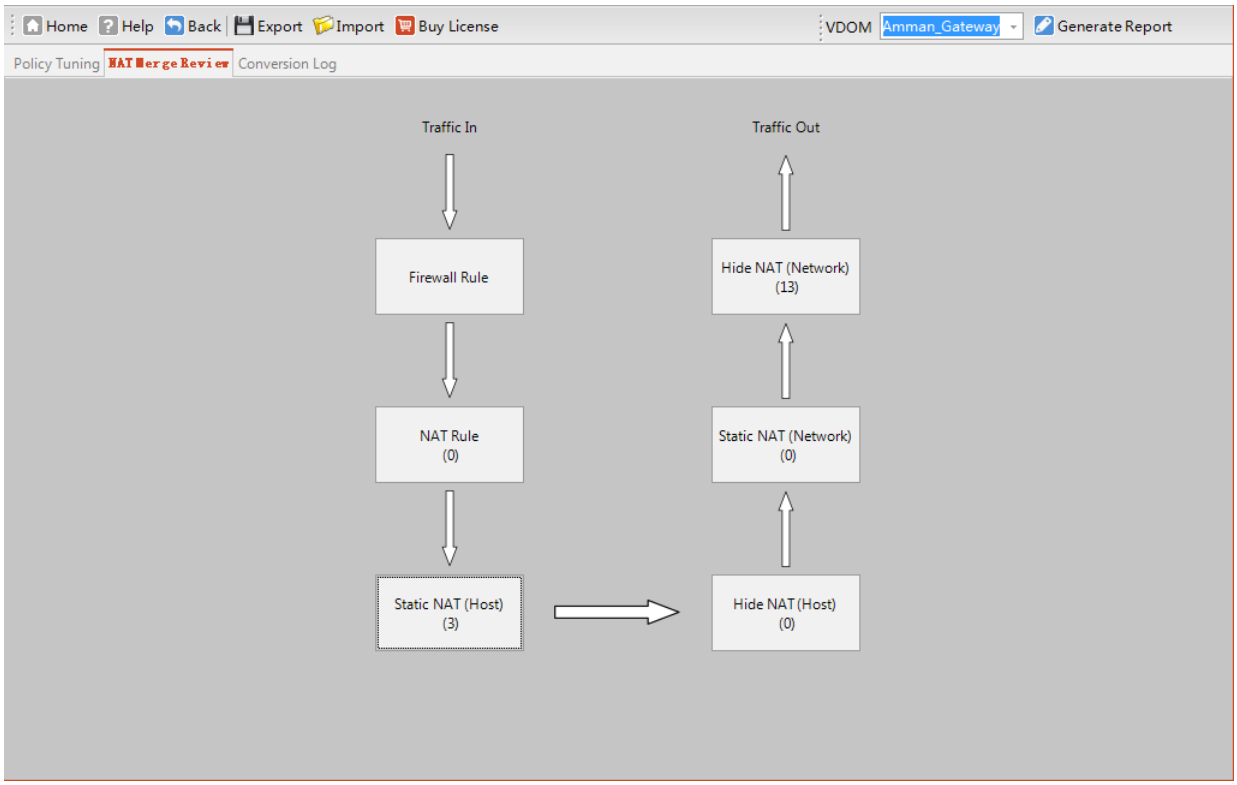
Policies that FortiConverter generated from a security rule from the source configuration have a five-digit name that is 10000 or higher .

Policies that FortiConverter generated by merging a NAT rule and security rule from the source configuration have a six-digit name that is 100000 or higher.

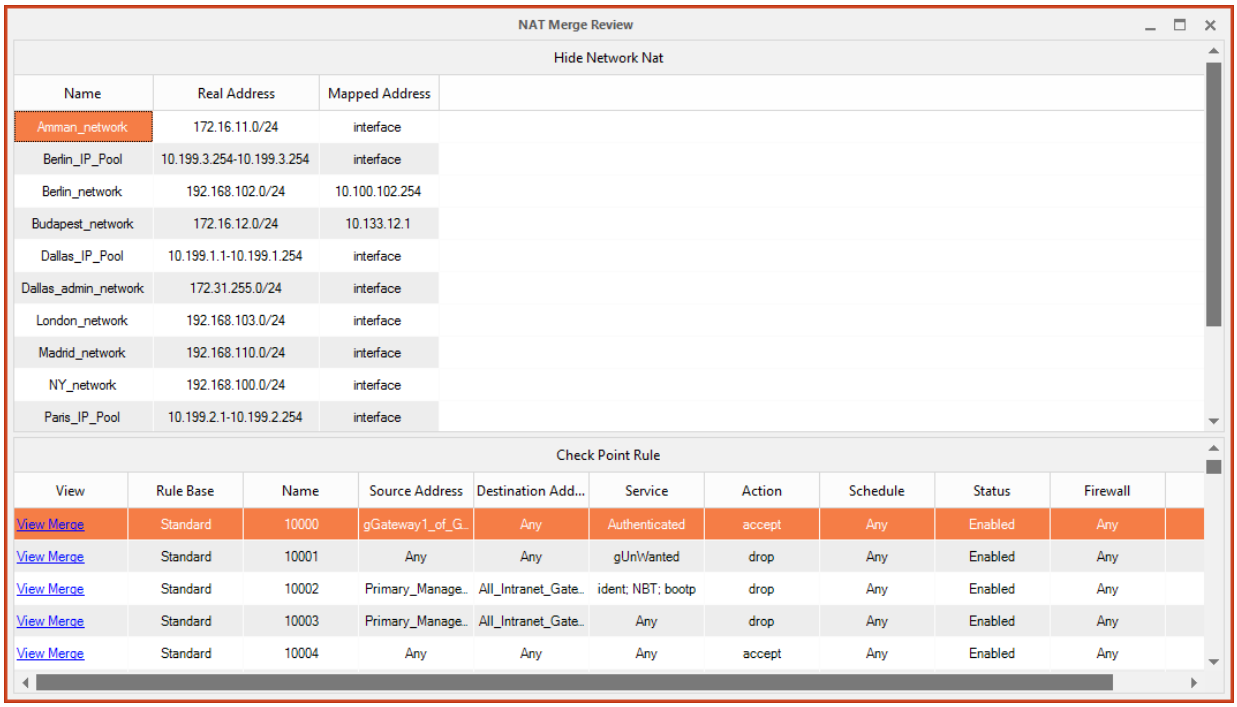
The Merge Summary provides a step-by-step description of the merge logic.

Check Point NAT Merge Review

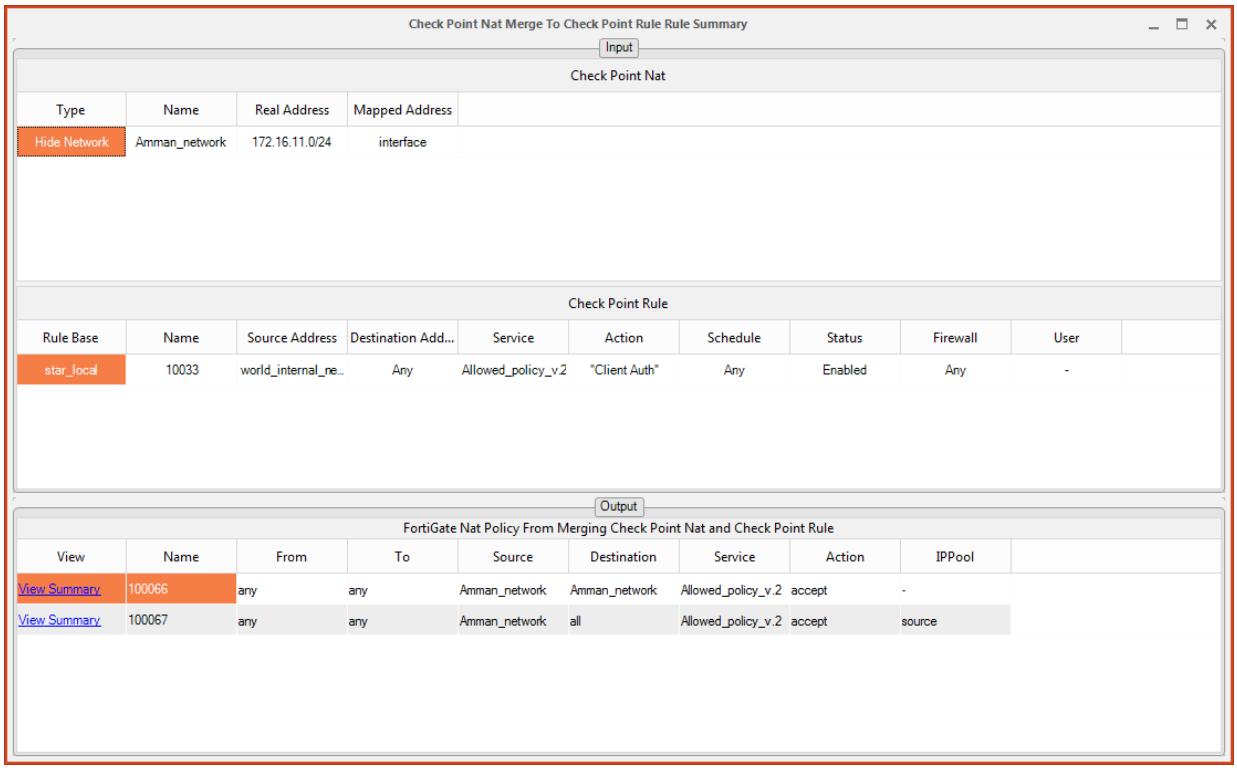
For Check Point, the NAT merge review tab displays the different NAT types as tiles in a diagram.



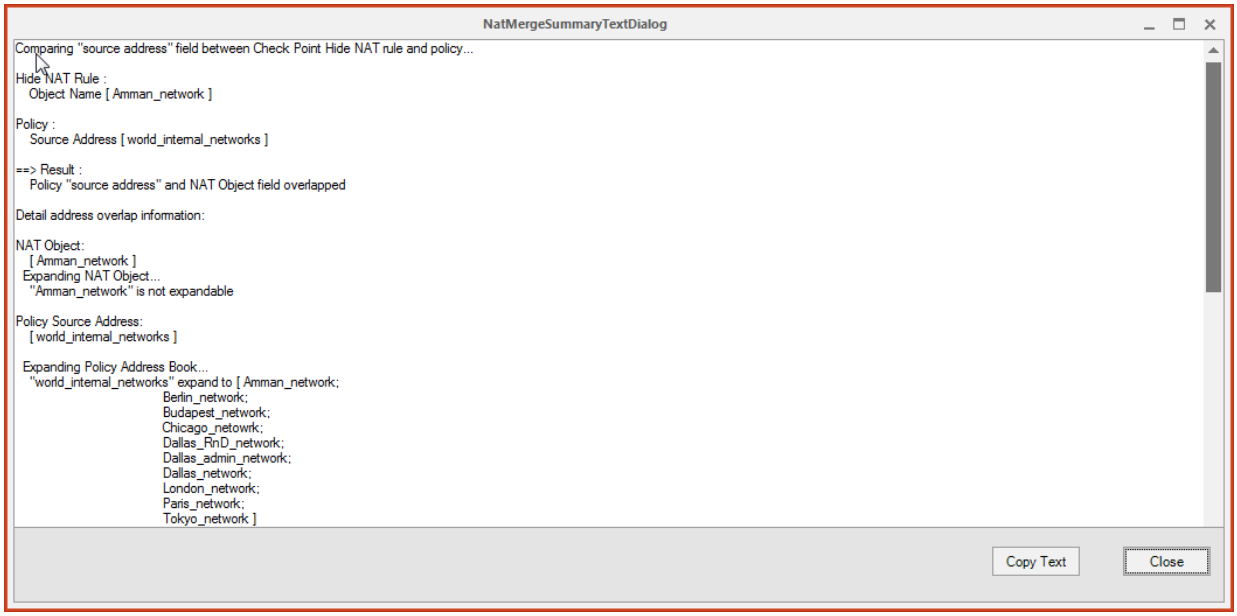
Click a tile to access the NAT rules and merge logs for that NAT type.



Click a network name, and then click **View Merge** to display detailed information about the input and output rules.

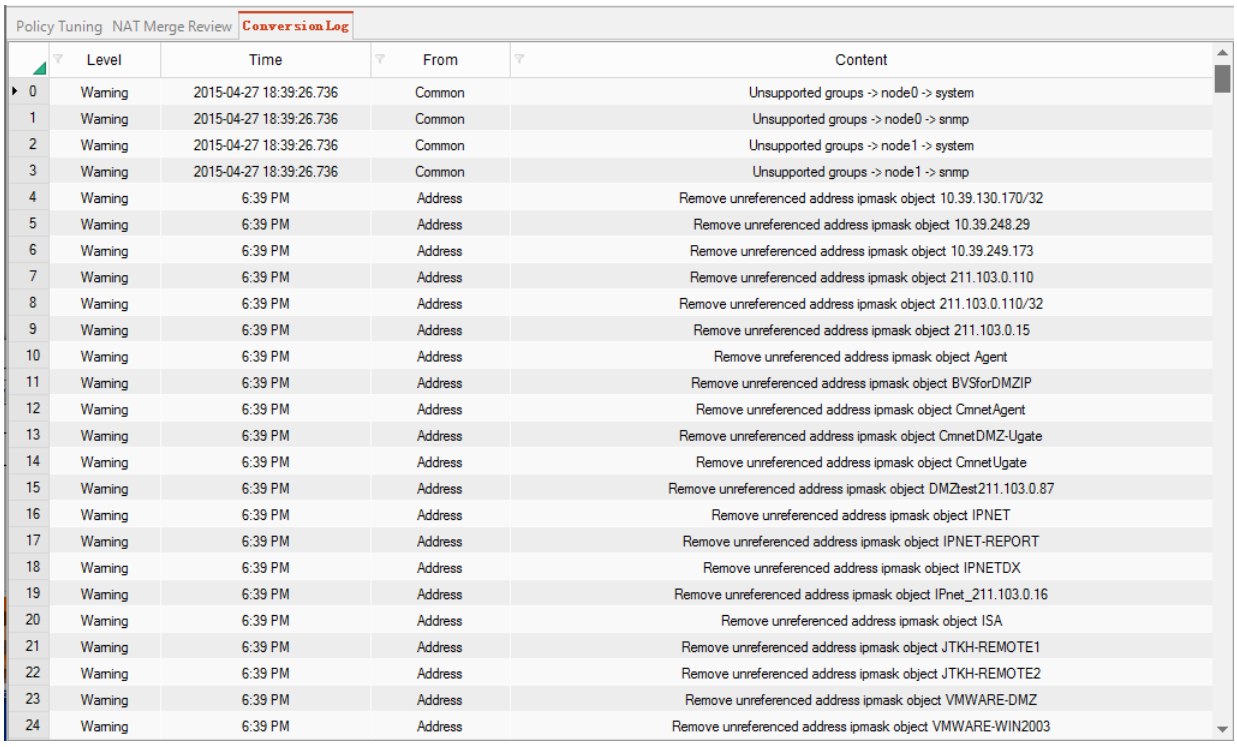


To view conversion log information about the merge, click **View Summary**.



Conversion log tab

The Conversion Log tab displays warnings that FortiConverter generated during the conversion process.



Policy Tuning | NAT Merge Review | Conversion Log

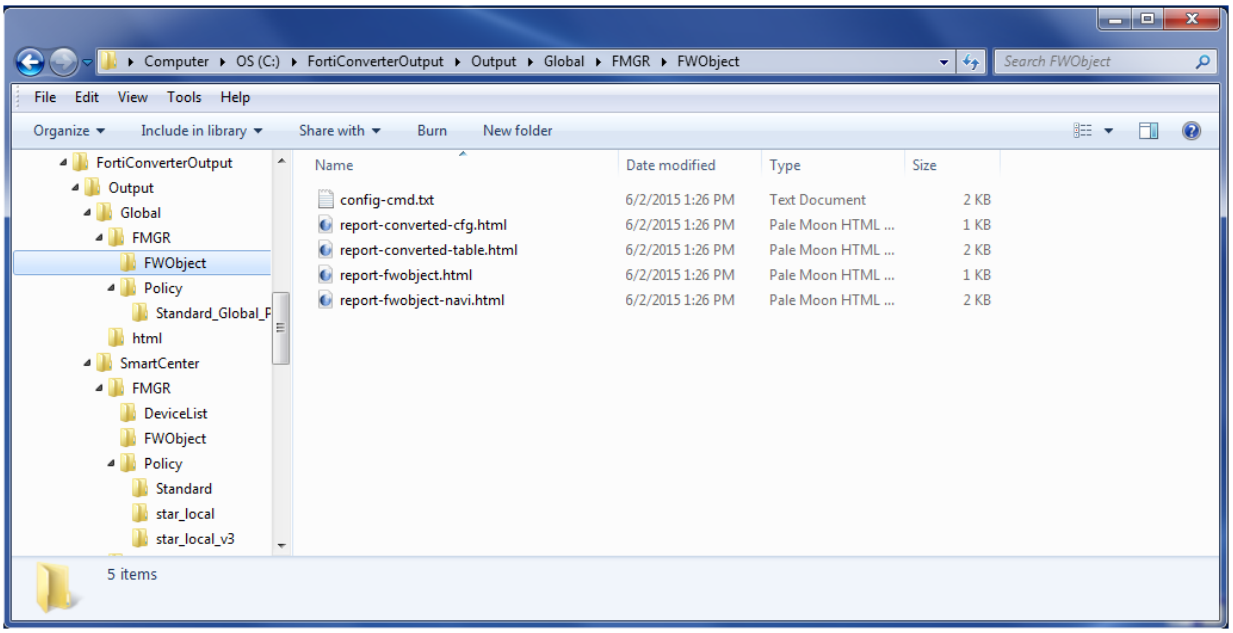
	Level	Time	From	Content
0	Warning	2015-04-27 18:39:26.736	Common	Unsupported groups -> node0 -> system
1	Warning	2015-04-27 18:39:26.736	Common	Unsupported groups -> node0 -> snmp
2	Warning	2015-04-27 18:39:26.736	Common	Unsupported groups -> node1 -> system
3	Warning	2015-04-27 18:39:26.736	Common	Unsupported groups -> node1 -> snmp
4	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 10.39.130.170/32
5	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 10.39.248.29
6	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 10.39.249.173
7	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 211.103.0.110
8	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 211.103.0.110/32
9	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 211.103.0.15
10	Warning	6:39 PM	Address	Remove unreferenced address ipmask object Agent
11	Warning	6:39 PM	Address	Remove unreferenced address ipmask object BVSforDMZIP
12	Warning	6:39 PM	Address	Remove unreferenced address ipmask object CmnetAgent
13	Warning	6:39 PM	Address	Remove unreferenced address ipmask object CmnetDMZ-Ugate
14	Warning	6:39 PM	Address	Remove unreferenced address ipmask object CmnetUgate
15	Warning	6:39 PM	Address	Remove unreferenced address ipmask object DMZtest211.103.0.87
16	Warning	6:39 PM	Address	Remove unreferenced address ipmask object IPNET
17	Warning	6:39 PM	Address	Remove unreferenced address ipmask object IPNET-REPORT
18	Warning	6:39 PM	Address	Remove unreferenced address ipmask object IPNETDX
19	Warning	6:39 PM	Address	Remove unreferenced address ipmask object IPnet_211.103.0.16
20	Warning	6:39 PM	Address	Remove unreferenced address ipmask object ISA
21	Warning	6:39 PM	Address	Remove unreferenced address ipmask object JTKH-REMOTE1
22	Warning	6:39 PM	Address	Remove unreferenced address ipmask object JTKH-REMOTE2
23	Warning	6:39 PM	Address	Remove unreferenced address ipmask object VMWARE-DMZ
24	Warning	6:39 PM	Address	Remove unreferenced address ipmask object VMWARE-WIN2003

Importing your new configuration into FortiManager

Output from conversion to FortiManager

After you convert a configuration to FortiManager, the output is organized in by source and type in multiple folders and text files.

For example, in the following illustration, the output files for a converted Checkpoint Provider-1 configuration are organized by source: Global and SmartCenter. They are further organized within each source by the following types: FWObject (network objects), Policy, and DeviceList (device configuration).The Policies folder contains a sub-folder for each source policy package.



Each FWObject and DeviceList folder and each Policy subfolder contains a config-cmd.txt. You use the contents of this text file to create FortiManager scripts that add the new configuration to your FortiManager instance.

To help you organized the import process and make troubleshooting easier, use a separate script for each config-cmd.txt. Alternatively, you can combine all the output files into a single script.

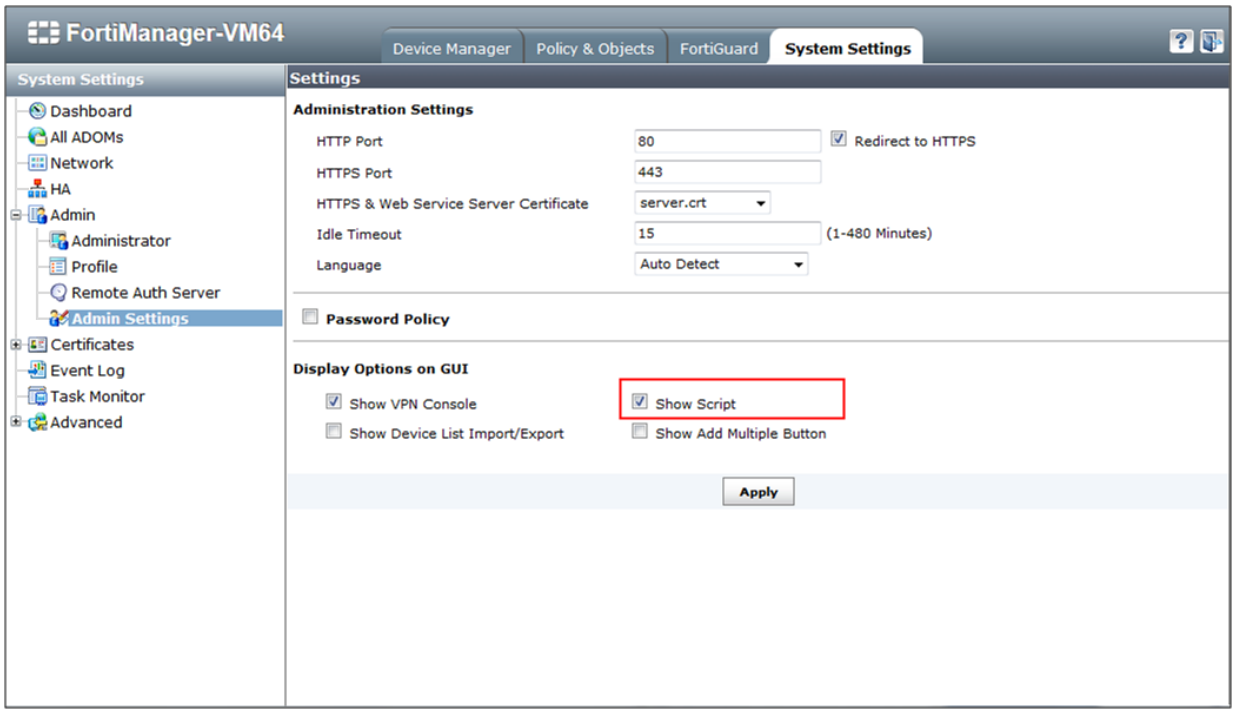
To avoid errors, run the scripts that you create using the contents of the FWObject folders first. If you use a single script, ensure that the commands from the FWObject folders come first in the script details. Policies that refer to an undefined object generate errors and interrupt the script.

Import your new configuration into FortiManager

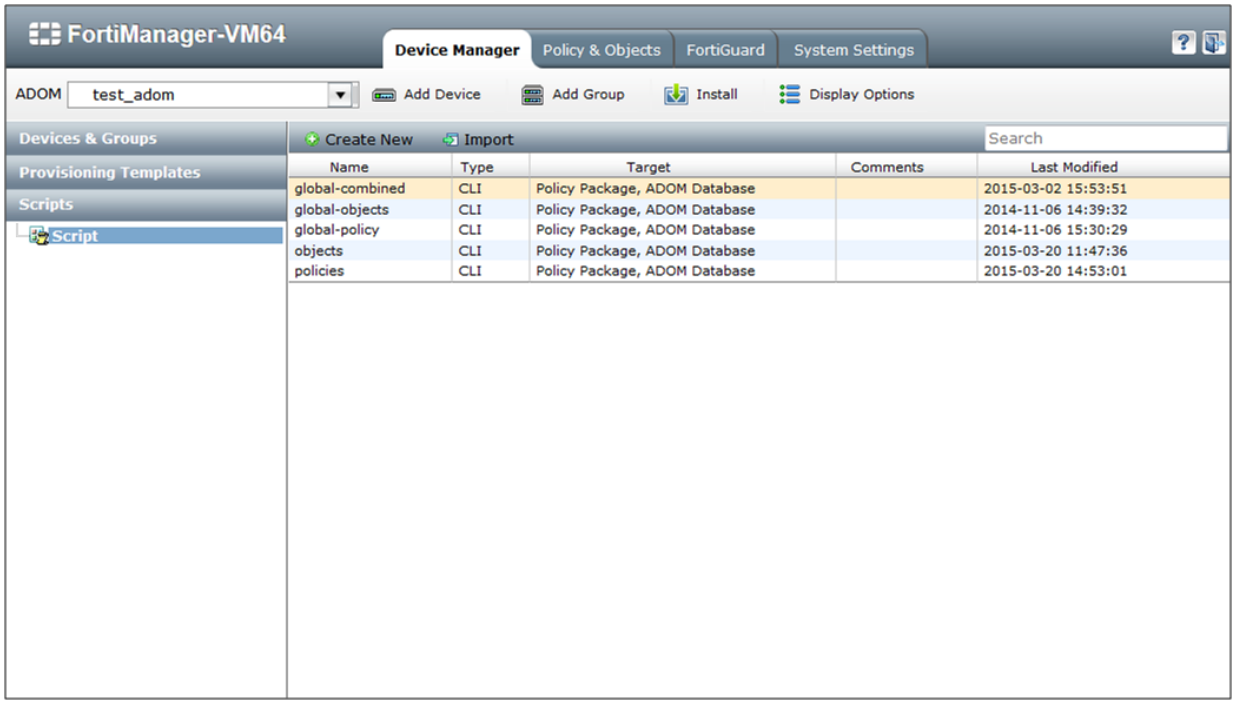
Object scripts should be run before policy scripts. Policies that refer to an undefined object generate errors and interrupt the script.

1. In FortiManager, go to **System Settings > Admin > Admin Settings**.

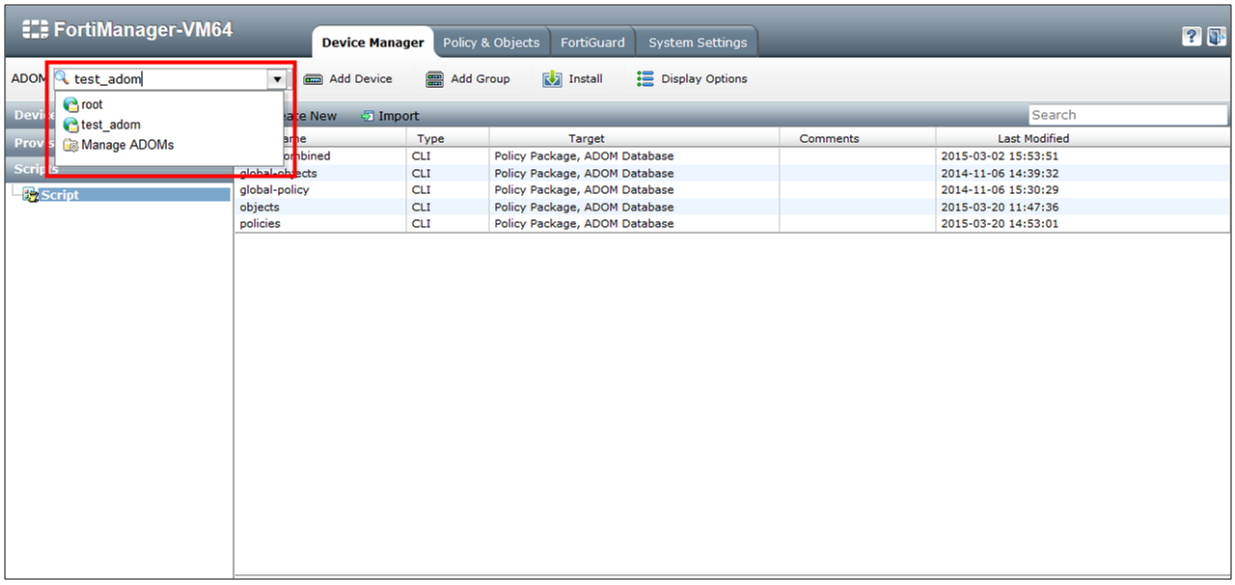
   Importing a converted configuration requires the scripting feature, which is hidden by default.
2. Select **Show Script**.



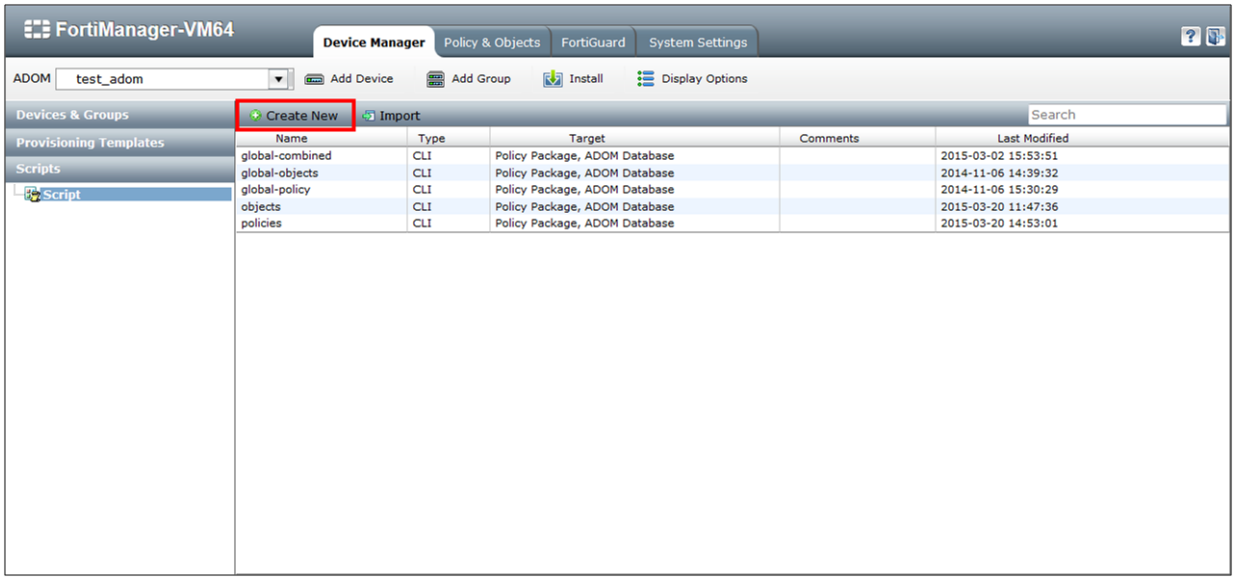
3. On the **Device Manager** tab, go to **Scripts > Script**.



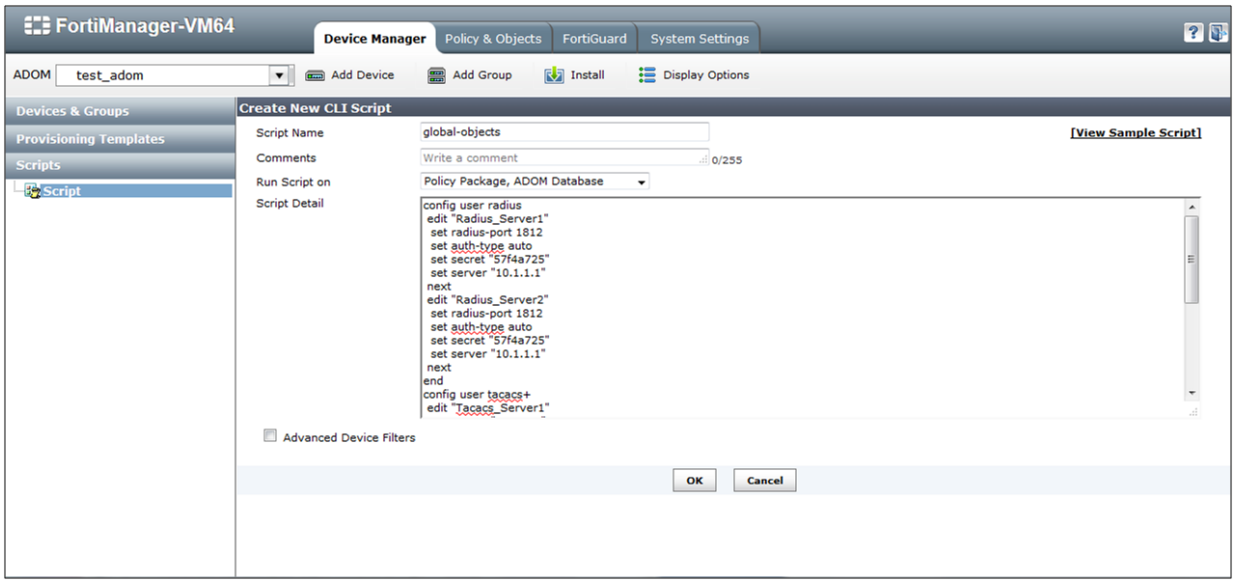
4. For **ADOM**, select the ADOM that you want to import the configuration into.



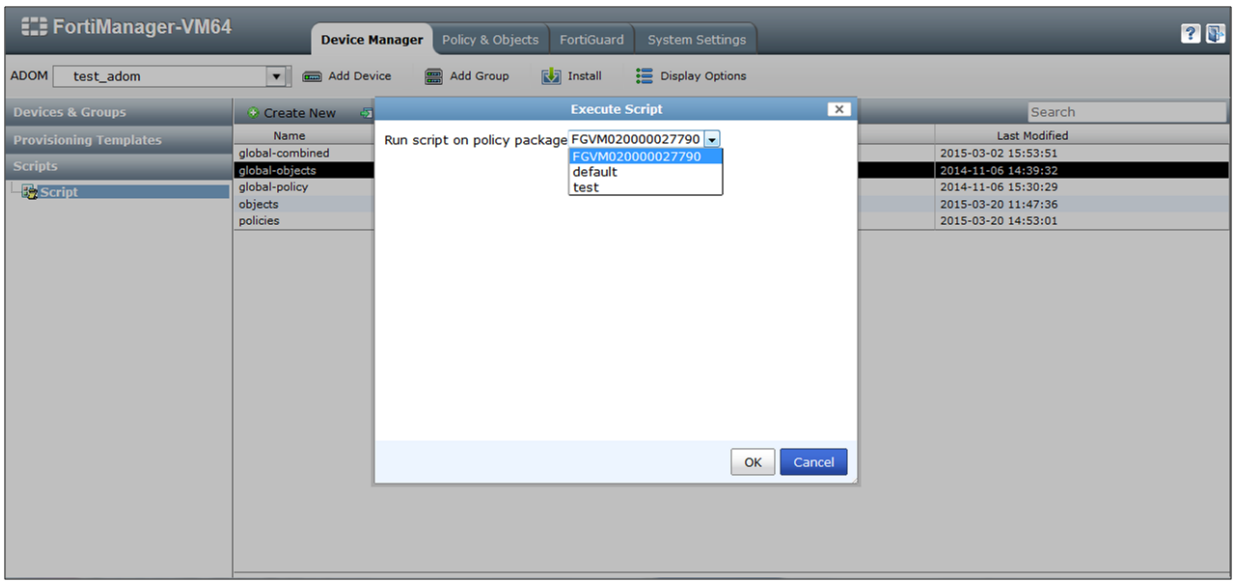
5. To create a new script, click **Create New**.



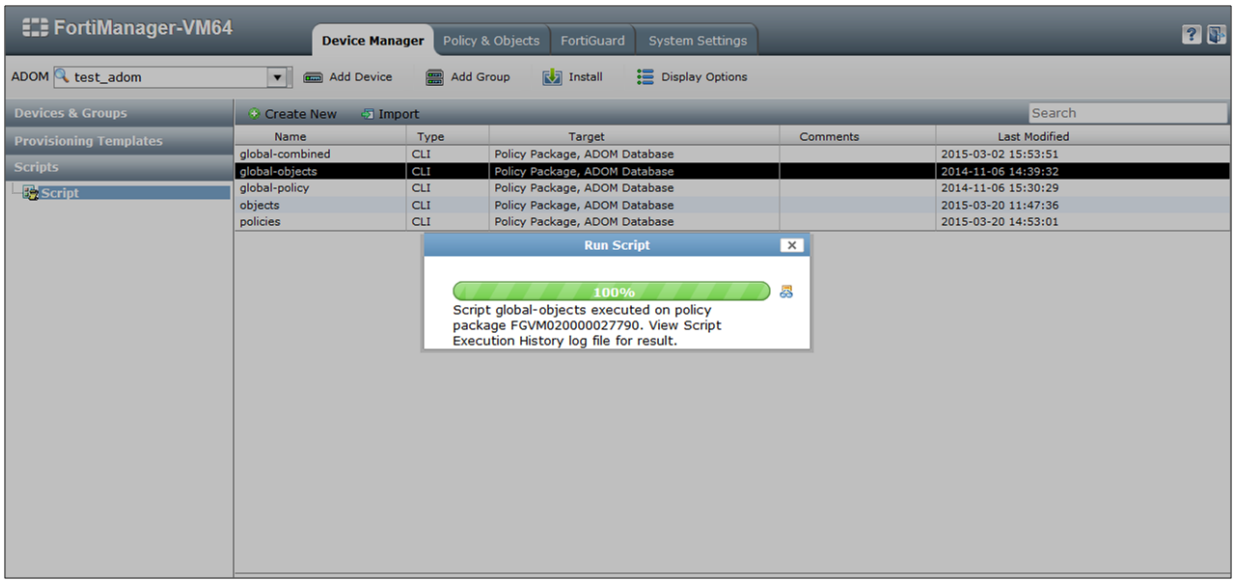
6. Enter a name for the script and for **Run Script on**, select **Policy Package, ADOM Database**.
7. For **Script Detail**, paste the content of one or more config-cmd.txt files.



8. Click **OK** to save the script.
9. In the list of scripts, right-click the script that you created, and then click **Run**.
10. For **Run script on policy package**, select a target, and then click **OK**.



A progress bar is displayed.



11. If you are importing the configuration using multiple scripts, repeat the script creation and run process for the remaining config-cmd.txt files.

Understanding your new configuration

To help you understand your new configuration, review the differences between FortiGate and FortiManager and your previous firewall.

Alcatel-Lucent differences

Conversion support

FortiConverter supports the conversion of the following Alcatel-Lucent Brick features:

- Interfaces
- Host Groups
- Service Groups
- Zone Brick Rulesets

Fortinet plans to support for the following Lucent features in a future FortiConverter release:

- NAT
- Schedule
- VPN
- Hosts Behind Zone

Address and address group configuration

- Lucent host addresses are mapped to FortiGate addresses.
- Lucent host groups are mapped to FortiGate address groups.
- Virtual Brick Addresses (VBA) are not supported.

Interface configuration

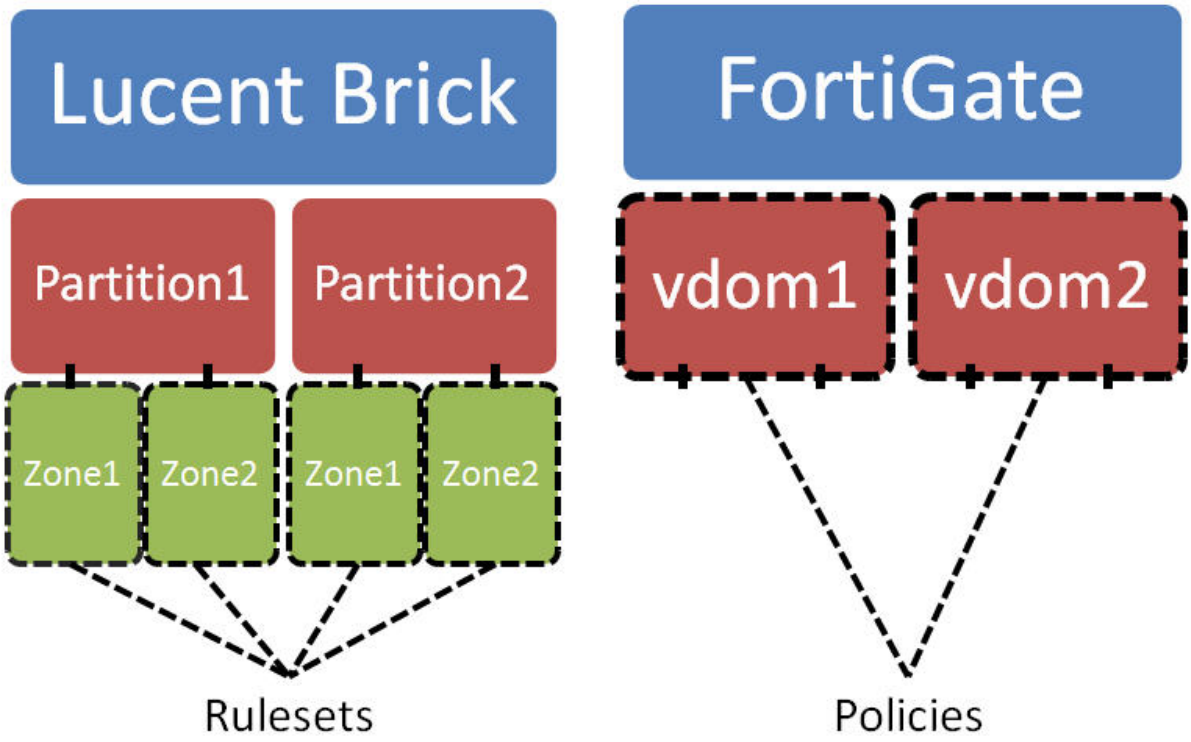
- FortiConverter assigns default VLAN configuration directly to physical interfaces.
- FortiConverter considers all VLANs named “*” or “Port Default”to be the default VLAN configuration.
- Domain Addresses are not supported.

Service and Service Group configuration

- Lucent Service Groups are mapped to FortiGate Service Groups.
- Lucent service “*” maps to FortiGate service “any”.

Policy configuration

Lucent Brick Zone Rulesets operate at the zone level, which has no direct equivalent in FortiGate. Zone rulesets need to be translated into equivalent FortiGate policies.



FortiConverter translates Lucent Brick rules by separating traffic into two categories: inter- partition and intra-partition.

- **Inter-partition traffic** behaves like inter-VDOM traffic, and is simple to convert to FortiGate policies.
- **Intra-partition traffic** is more complicated to convert because multiple zone rules can be applied.

FortiConverter handles the inter-partition traffic by creating a general policy for each rule.

FortiConverter handles the intra-partition traffic by looking for all matches between two zone rulesets. FortiConverter looks at 3 fields: source, destination, and service. All 3 fields must overlap for the rules to match. FortiConverter creates a policy for each match using the intersection of each field.

The action of the rules determines the action of the converted policy, as shown in the following table:

Rule 1	Rule 2	Policy
Pass	Pass	Accept
Pass	Drop	Deny
Drop	Pass	Deny
Drop	Drop	Deny

Inter-partition Deny policies have higher priority than intra-partition policies, while inter- partition Accept policies have lower priority than intra-partition policies.

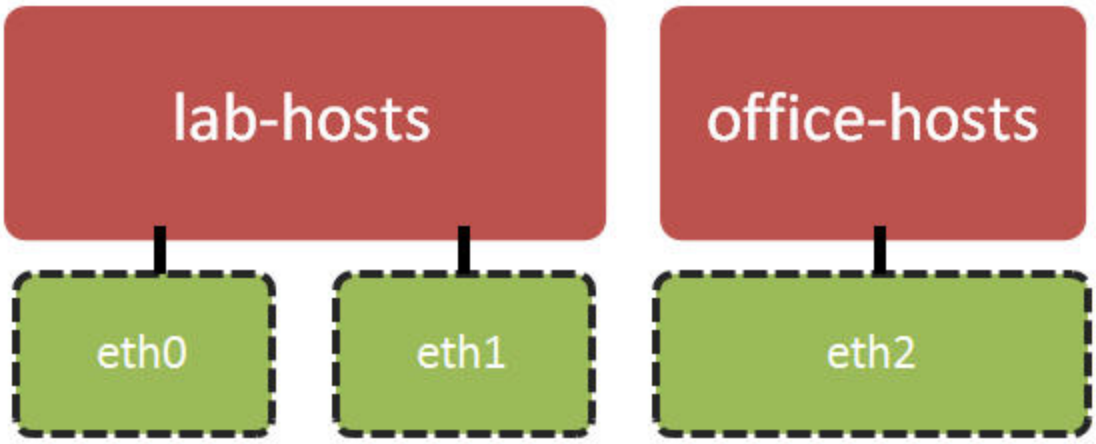
Lucent default rulesets “firewall” and “administrativezone” are currently unsupported.

VDOM configuration

- Lucent partitions map to FortiGate VDOMs.
- VDOM names are limited to 11 characters. FortiConverter truncates longer names to 11 characters.
- Lucent partition “*Default” maps to the FortiGate root VDOM.

Example conversion

The following block diagram and tables illustrates a Lucent configuration with 2 partitions and 3 zones.

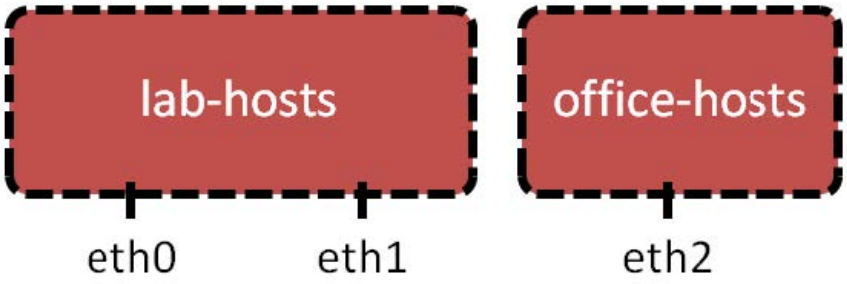


Zone eth0 Ruleset					
Rule Num	**Direction**	**Source**	**Destination**	**Service**	**Action**
1000	Out	192.168.1.15	172.30.10.1/24	*	Drop
1001	Both	192.168.1.0/24	172.30.10.1/24	*	Pass

Zone eth1 Ruleset					
Rule Num	**Direction**	**Source**	**Destination**	**Service**	**Action**
1000	In	*	172.30.10.5 - 172.30.10.20	TCP	Pass
1001	Both	192.168.1.132	172.30.10.9	*	Pass

Zone eth2 Ruleset					
Rule Num	**Direction**	**Source**	**Destination**	**Service**	**Action**
1000	Both	*	10.10.15.0/24	HTTP	Pass

This Lucent configuration creates the following FortiGate configuration. Inter-partition rules are in **bold**.



VDOM lab-hosts Policies						
Policy Num	**Src Interface**	**Dst Interface**	**Source**	**Destination**	**Service**	**Action**
10000	**eth0**	**any**	**192.168.1.15**	**172.30.10.1/24**	*	**Deny**
10001	eth0	eth1	192.168.1.0/24	172.30.10.5 - 172.30.10.20	TCP	Accept
10002	eth0	eth1	192.168.1.132	172.30.10.9	*	Accept
10003	**eth0**	**any**	**192.168.1.0/24**	**172.30.10.1/24**	*	**Accept**
10004	any	eth0	192.168.1.0/24	172.30.10.1/24	*	Accept
10005	eth1	eth0	192.168.1.132	172.30.10.9	*	Accept
10006	**eth1**	**any**	**192.168.1.132**	**172.30.10.9**	*	**Accept**
10007	**any**	**eth1**	**192.168.1.132**	**172.30.10.9**	*	**Accept**

VDOM office-hosts Policies						
Policy Num	**Src Interface**	**Dst Interface**	**Source**	**Destination**	**Service**	**Action**
10000	**any**	**eth2**	**any**	**10.10.15.0/24**	**HTTP**	**Accept**
10001	**eth2**	**any**	**10.10.15.0/24**	**any**	**TCP**	**Accept**

Check Point differences

General

- FortiGate's `set allowaccess` command for interfaces does not exist on Check Point. Because FortiGate requires this setting, FortiConverter by default enables all services for interfaces.
- The interface "Lead to Internet" is a default static route on FortiGate.

Schedule configuration

FortiConverter converts "Day in month" time schedules to FortiGate one-time schedules. It converts "Day in week" and "None" schedules to recurring schedules.

You assign a year range for the "Day in month" schedule. If the specified day does not exist for a certain month, FortiConverter does not generate the one-time schedule for that month.

For example, the Check Point firewall's "Day in month" time schedule has the following parameters for each year:

```
Month: Jan/March/Sept.
Day: 1, 5, 31
Start and end time: 0:00 to 10:00
```

If you select `1` for **Convert 'Day in Month' to 'One Time Schedule' for next x years** in the FortiConverter conversion wizard and the current year value for the PC running FortiConverter is 2013, the wizard generates the following output for FortiGate one-time schedules:

```
From 0:00 Jan/1/2013 To 10:00 Jan/1/2013
From 0:00 Jan/5/2013 To 10:00 Jan/5/2013
From 0:00 Jan/31/2013 To 10:00 Jan/31/2013
From 0:00 Match/1/2013 To 10:00 Match/1/2013
From 0:00 Match/5/2013 To 10:00 Match/5/2013
From 0:00 Match/31/2013 To 10:00 Match/31/2013
From 0:00 Sept./1/2013 To 10:00 Sept./1/2013
From 0:00 Sept./5/2013 To 10:00 Sept./5/2013
```

Notice that FortiConverter does not generate a Sept. 31 schedule.

NAT and policy configuration

- In Check Point, static NAT is a 1-to-1 IP relationship. In the FortiGate NAT policy found in the converted configuration, source NAT with an IP pool is not a 1-to-1 relationship.
- FortiConverter converts rule actions with "Client Auth" to FortiGate user-identity policies with the "Accept" action.
- FortiConverter does not convert NAT global properties.

VPN configuration

- Check Point does not configure VPN within a firewall rule. When FortiConverter converts the configuration to FortiGate, it generates several VPN policies from non-"Lead to Internet" interfaces to the "Lead to Internet" (default route) interface.
- After FortiConverter converts the VPN configuration, the VPN policy's destination interface refers to the "Lead to Internet" interface.

  If you changed the default route's egress interface, you may need to update the VPN/Policy configuration manually.

Service objects

Unlike FortiGate service objects, Check Point service objects have a protocol type attribute. FortiGate uses a session helper object to provide the same functionality as the service objects with a protocol type attribute.

Cisco IOS, PIX or ASA differences

- FortiGate's `set allowaccess` command for interfaces does not exist on Cisco firewalls. Because FortiGate requires this setting, FortiConverter by default enables all services for interfaces.
- Cisco `object-group` objects have two types of service definitions. Because FortiGate services have both a source and destination port, FortiConverter can only convert `service-object` items into FortiGate services. By default, it does not convert the other type of service object, defined by `port- object`. FortiConverter generates FortiGate service objects from a Cisco ACL's protocol and source/destination port.
- On Cisco IPSec VPNs, Phase 1 (ISAKMP) supports more than two types of authentication methods. FortiGate supports only two types: `pre-share` and `rsa-sig`. Therefore,you must assign methods for each VPN connection. The wizard converts Cisco EZVPN configuration to FortiGate VPN policies from the "Intranet" interface to the interface which was assigned by the `crypto map interface` command.
- FortiConverter does not support the following Cisco configuration elements:
  - ASA objects for NAT and double NAT
  - Identity NAT and NAT Exemption
  - Wild card netmasks for `access-list` and `object- group` objects
  - EZVPN conversion

    For example, FortiConverter does not support `crypto ipsec profile <profile-name>` and `crypto isakmp profile <profile-name>` .
  - To reduce the number of NAT polices a conversion generates, FortiConverter does not convert Static NAT rules in which the source and mapped IPs are the same.

"FortiConverter supports Static NAT, Policy NAT, Dynamic NAT, and PAT. Identity NAT and NAT Exemption are not supported. Static NAT also supports identity translation - where the source and mapped are the same, these rules are not converted, reducing the number of NAT polices generated by the conversion.

Juniper ScreenOS or Junos OS differences

- FortiConverter recognizes interface names starting with "vlan" as logical interfaces.
- Junos service objects support MS-RPS and SUN-RPC, where program-numbers (SUN) and UUID (MS) are used instead of ports. FortiOS supports this configuration using Application Control with an application override.

Example of Junos service object conversion

```
config application list
 edit "MS-ActiveDirectory"
  config entries
   edit 1
    set application 152305667
     config parameters
      edit 1
       set value "45f52c28-7f9f-101a-b52b-08002b2efabe"
      next
      edit 2
       set value "811109bf-a4e1-11d1-ab54-00a0c91e9b45"
      next
     end
    set action pass
   next
  end
 next
end

edit 10012
  set srcintf "trust"
  set dstintf "mgn"
  set srcaddr "MEI-Novi-172.24.81.0-24" "MEI-Novi-172.24.80.0-24" "MEI-Novi-
172.24.252.112-28"
  set dstaddr "MEI-WAN"
  set service "MS-ActiveDirectory"
  set schedule "always"
  set logtraffic all
  set status enable
  set action accept
  set comments "95"
  set application-list "MS-ActiveDirectory"
 next
```

Palo Alto Networks OS (PAN-OS) differences

Conversion support

FortiConverter does not support the following features

- VPN
- IPv6 address ranges
- IPv6 address subnets (will be supported in a future release)
- UTM

Configuration notes

- PAN-OS handles NAT and firewall policies with two separate modules, while FortiGate handles NAT within its policy module. FortiConverter makes a best effort attempt to map NAT rules onto each policy during the conversion, but you should review the results for accuracy.
- FortiConverter converts PAN-OS weekly schedules to FortiGate weekday schedules that are stored in a schedule group.

High Performance Network Security